Agility 2018 Hands-on Lab Guide

Contents:

1 Introduction

In this lab session, you will be introduced to a few different ways to gather, visualize and analyze traffic information available on a BIG-IP platform. It is assumed that you are familiar with the basics of setting up a BIG-IP device for various ADC functions. The lab environment has already been setup with an HA pair of BIG-IP Virtual Editions (VEs) that have been pre-configured for a few web applications. Your task will be to configure the BIG-IPs to generate Analytics data so that you may visualize and analyze this data.

1.1 Lab Environment Setup

The following components have been setup with basic configurations for you:

- 2x **F5 BIG-IP VEs** running version 13.1.0.5, paired in an Active/Standby HA Cluster
- 1x **Linux LAMP Server** running Splunk and a few different web applications
- 1x **Windows jumphost**

1.2 Accessing the Lab Environment

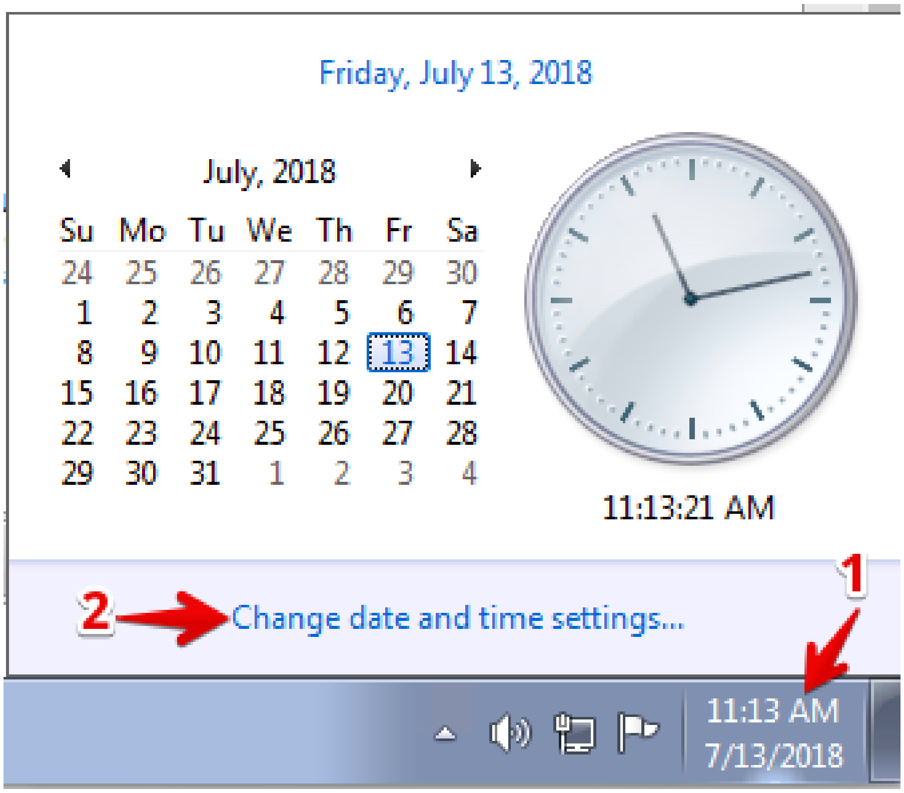
To access the lab environment, you will require a web browser and Remote Desktop Protocol (RDP) client software. The web browser will be used to access the Lab Training Portal to retrieve the IP address for your Windows jump host that you will RDP into to access the entire lab environment.

Note: All work for this lab will be performed exclusively from the Windows jumphost. No installation or interaction with your local system is required.

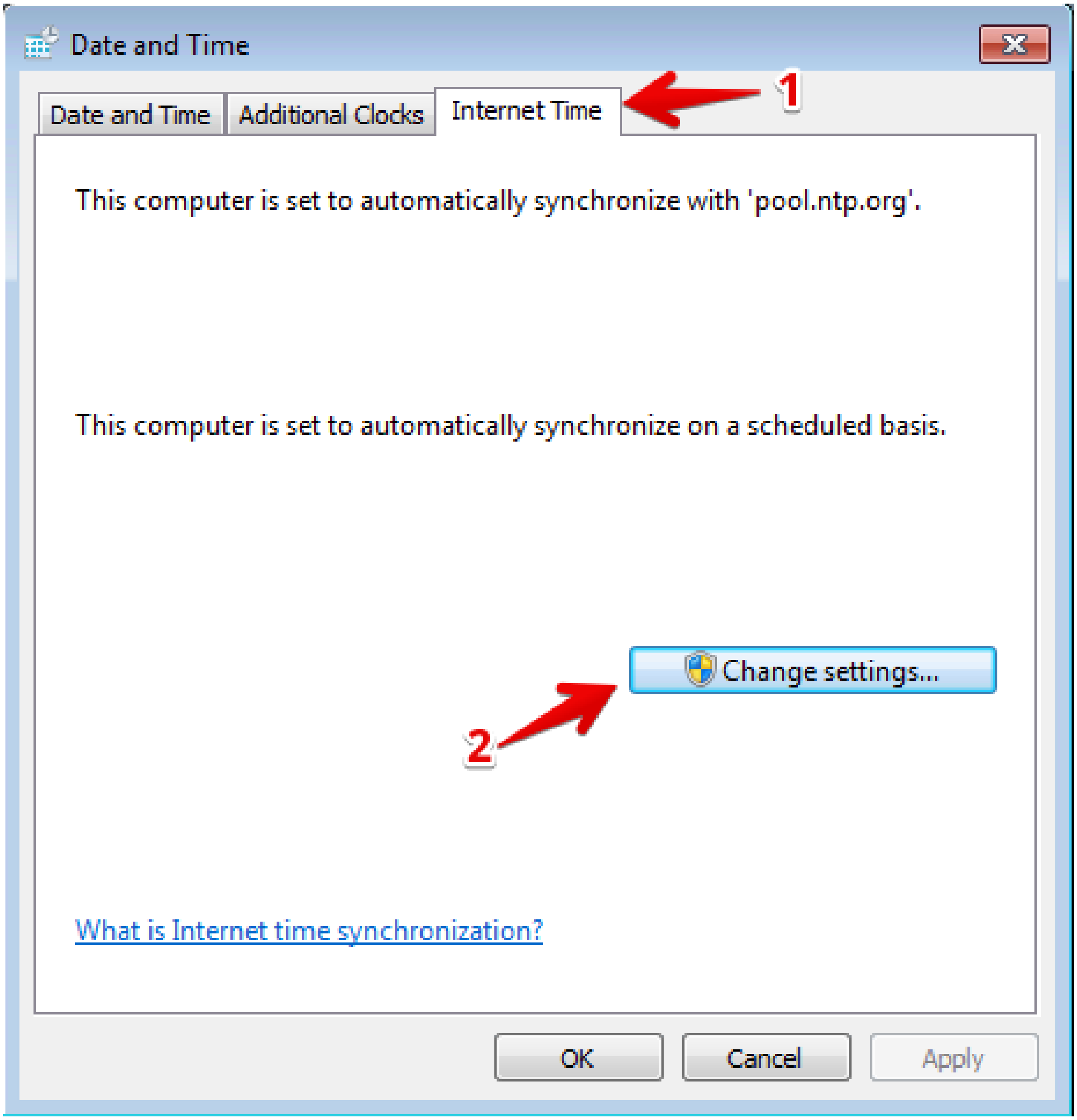
- Connect to the Training Portal (details provided by lab instructor)
- Retrieve the IP address / hostname of the Windows jumpbox (Win7 Client)
- Establish an RDP connection to your jumpbox and login with the following credentials:
  - User: `external_user`
  - Password: `F5Agility`

Ignore any warnings about Windows activation

- Ensure that the Windows jumpbox has the correct time. This is necessary in order for other operations to work correctly. To set the correct time, click on the Date/Time in the bottom right-hand corner of the RDP window, and then click on **Change date and time settings**

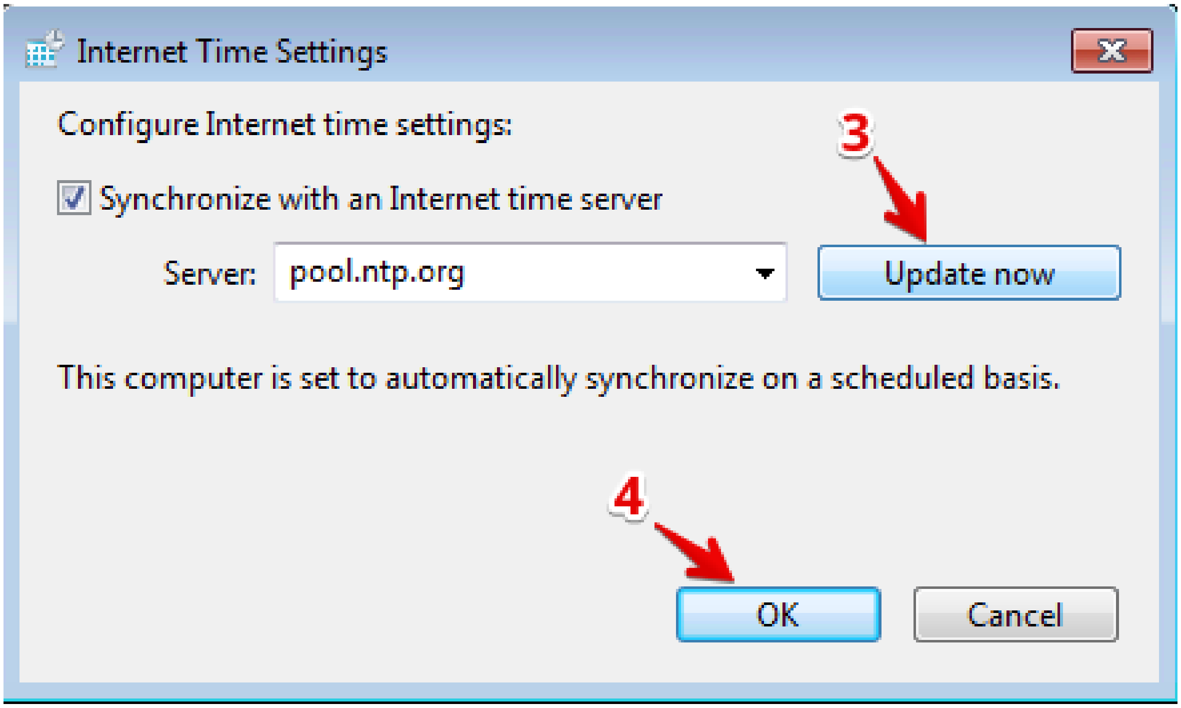


- In the **Date and Time** window:
  1. Click on the **Internet Time** tab
  2. Click **Change settings. . .**
  3. Then click **Update now.**
  4. Finally, click **OK**, and **OK** one more time



This computer is set to automatically synchronize with 'pool.ntp.org'.

This computer is set to automatically synchronize on a scheduled basis.



Internet Time Settings

Configure Internet time settings:

☑ Synchronize with an Internet time server

Server: pool.ntp.org

This computer is set to automatically synchronize on a scheduled basis.

2

Lab 1 - Introduction to AVR

The **Application Visibility and Reporting (AVR)** module provides detailed charts and graphs to give you more insight into the performance of web applications, with detailed views on HTTP and TCP stats, as well as system performance (CPU, memory, etc.). You can use this module to visualize the traffic being processed by your BIG-IP device, and gain a better understanding of where the traffic is originating from (client IP addresses / subnets as well as geographical regions), the nature and volume of request and response traffic (Total Transactions as well as Average and Max Transactions/sec), the most commonly requested URLs, Server Latency and Page Load times, Virtual Server and Pool member performance, and many more metrics.

This lab will give you an introduction on how to setup the AVR module to generate these charts / reports and how to visualize them on your BIG-IP.

Note: The AVR module is a built-in module that is included at no charge with all BIG-IP licenses for software versions 11.x and higher. However, this module is not enabled by default since it consumes additional resources. Hence you must make the conscious decision to provision the module and enable analytics data collection on the Virtual Servers of interest. In your own production environment, you may want to start with enabling analytics data collection on a handful of virtual servers and observe the impact to system performance before enabling it on a larger number of virtual servers.

2.1 Configuring AVR to generate on-box Analytics reports

In this lab, you will first configure an Analytics profile to attach to your existing applications (Virtual Servers). You will then view the analytics graphs and charts on the BIG-IP to gain more insight into the traffic patterns for incoming traffic for your applications.

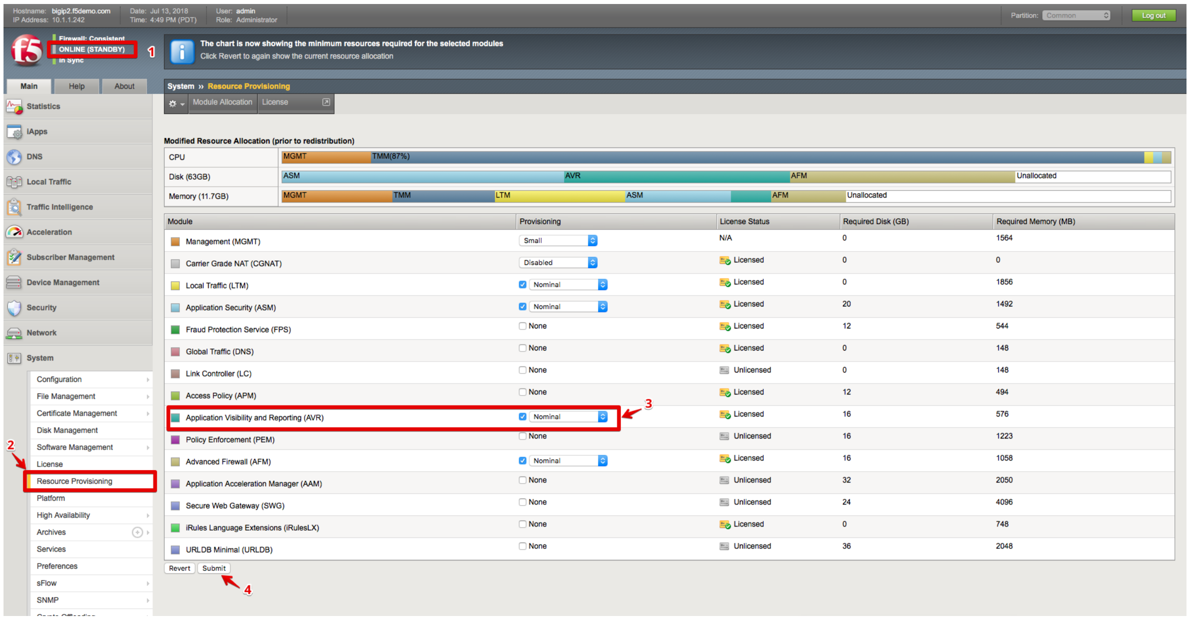
Note: You will perform all configuration tasks from the Windows jump box

1. On the Windows Jump box, open the Chrome browser, and then use the bookmarks in the bookmark bar to access **BIGIP_1** and **BIGIP_2** in separate tabs. If you get a warning about an invalid SSL certificate, ignore the warning, and continue to the login page.
2. Login to both BIG-IPs with these credentials:
    - username: `admin`

- password: `Agility2018`

2.1.1 Task 1 – Provision the AVR module

1. Determine which BIG-IP is the standby unit by looking at the status in the top-left corner of each of the BIG-IP GUI windows. Normally BIGIP2 should be the standby, but in some cases, you may find that BIGIP1 is the standby unit.
2. First, on the standby unit, go to **System >> Resource Provisioning**
3. For the **Application Visibility and Reporting (AVR)** module, check-mark the box under the **Provisioning** column, and ensure the Provisioning level is set to **Nominal**.
4. Click **Submit**



The chart is now showing the minimum resources required for the selected modules
Click Revert to again show the current resource allocation

Modified Resource Allocation (prior to redistribution)

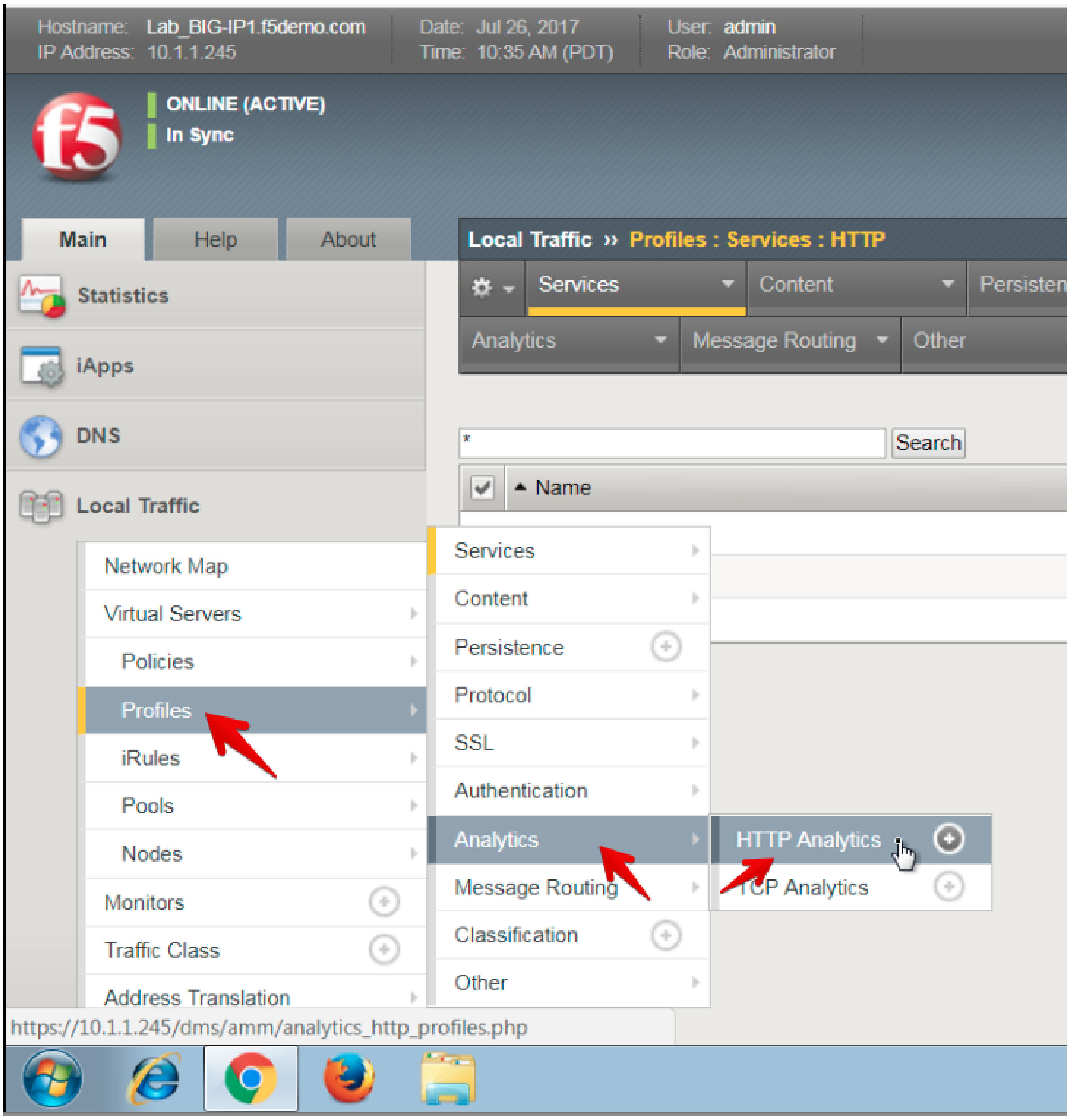
Module	Provisioning	License Status	Required Disk (GB)	Required Memory (MB)
Management (MGMT)	Small	N/A	0	1564
Carrier Grade NAT (CGNAT)	Disabled	Licensed	0	0
Local Traffic (LTM)	☑ Nominal	Licensed	0	1856
Application Security (ASM)	☑ Nominal	Licensed	20	1492
Fraud Protection Service (FPS)	□ None	Licensed	12	544
Global Traffic (DNS)	□ None	Licensed	0	148
Link Controller (LC)	□ None	Unlicensed	0	148
Access Policy (APM)	□ None	Licensed	12	494
Application Visibility and Reporting (AVR)	☑ Nominal	Licensed	16	576
Policy Enforcement (PEM)	□ None	Unlicensed	16	1223
Advanced Firewall (AFM)	☑ Nominal	Licensed	16	1058
Application Acceleration Manager (AAM)	□ None	Unlicensed	32	2050
Secure Web Gateway (SWG)	□ None	Unlicensed	24	4096
iRules Language Extensions (iRulesLX)	□ None	Licensed	0	748
URLDB Minimal (URLDB)	□ None	Unlicensed	36	2048

Note: This procedure will cause services to be restarted on the BIG-IP and may cause interruption to the traffic that is passing through the unit. Hence, it is always recommended to perform this step during a maintenance window, and to start with the Standby unit first.

5. Once the services have been restarted, click **Continue**.
6. Repeat the above steps for the other (Active) BIG-IP unit. Note that when you do so, the Active unit will go into Standby state, and the other unit will take over as Active.

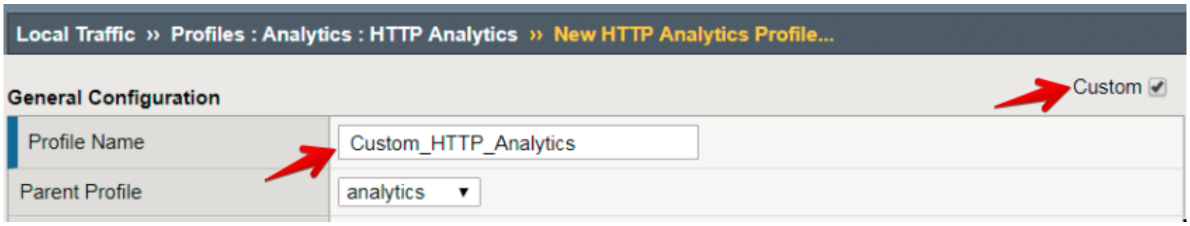
2.1.2 Task 2 – Create a new Analytics profile and attach it to your Virtual Servers

1. On the Active unit, go to **Local Traffic >> Profiles >> Analytics >> HTTP Analytics**



Hostname: Lab_BIG-IP1.f5demo.com
IP Address: 10.1.1.245
Date: Jul 26, 2017
Time: 10:35 AM (PDT)
User: admin
Role: Administrator

2. Click **Create**
3. Click the **Custom** checkbox in the top-right
4. Type in **Custom_HTTP_Analytics** for the **Profile Name**



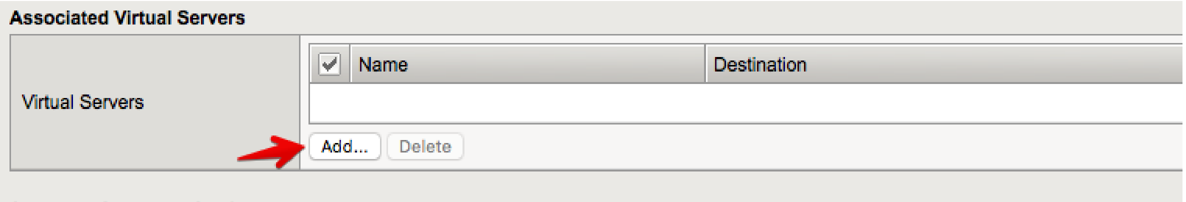
Local Traffic » Profiles : Analytics : HTTP Analytics » New HTTP Analytics Profile...

General Configuration — Custom ☑

Profile Name	Custom_HTTP_Analytics
Parent Profile	analytics ▾

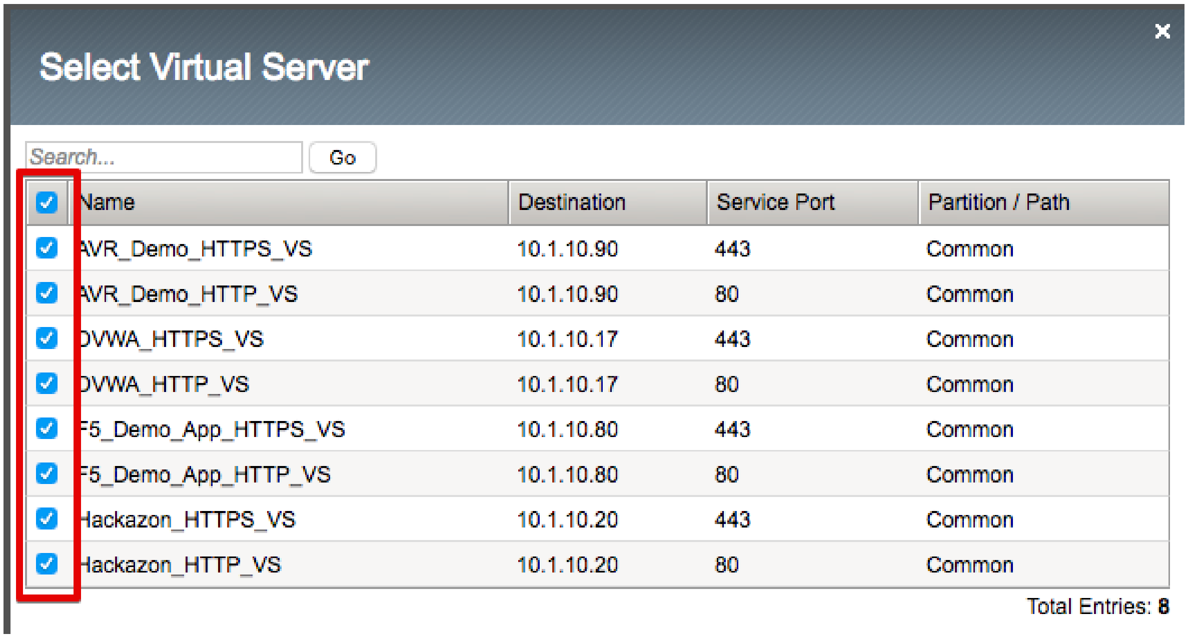
5. Under the **Associated Virtual Servers** section, click **Add**, and then select all listed Virtual Servers. This will add this profile to all the virtual servers simultaneously without having to individually modify

each virtual server.



Associated Virtual Servers

Virtual Servers	☑ Name	Destination

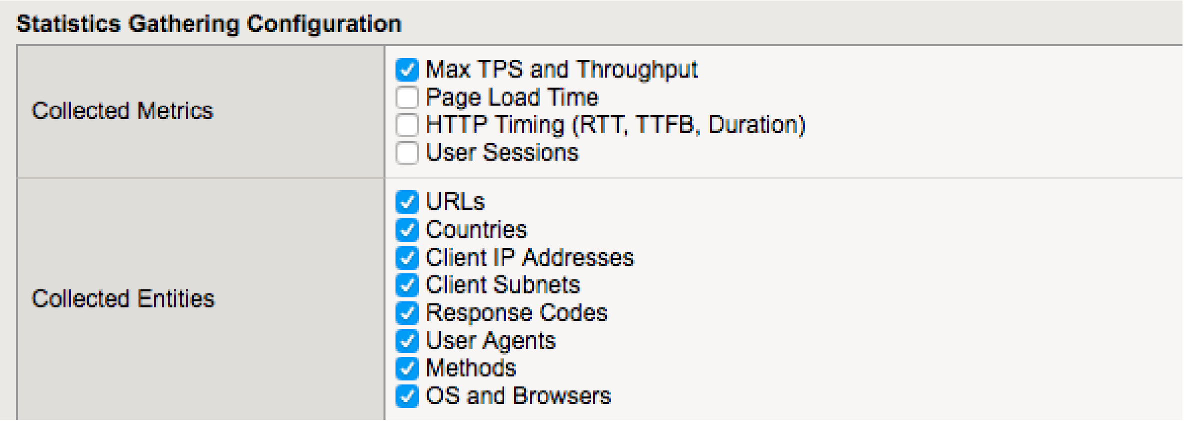


Select Virtual Server

☑	Name	Destination	Service Port	Partition / Path
☑	AVR_Demo_HTTPS_VS	10.1.10.90	443	Common
☑	AVR_Demo_HTTP_VS	10.1.10.90	80	Common
☑	DVWA_HTTPS_VS	10.1.10.17	443	Common
☑	DVWA_HTTP_VS	10.1.10.17	80	Common
☑	F5_Demo_App_HTTPS_VS	10.1.10.80	443	Common
☑	F5_Demo_App_HTTP_VS	10.1.10.80	80	Common
☑	Hackazon_HTTPS_VS	10.1.10.20	443	Common
☑	Hackazon_HTTP_VS	10.1.10.20	80	Common

Total Entries: **8**

6. Under the **Statistics Gathering Configuration,** checkmark the following options:
   - **Max TPS and Throughput**
   - **URLs**
   - **Countries**
   - **Client IP Addresses**
   - **Client Subnets**
   - **Response Codes**
   - **User Agents**
   - **Methods**
   - **OS and Browsers**



Statistics Gathering Configuration

Collected Metrics	☑ Max TPS and Throughput □ Page Load Time □ HTTP Timing (RTT, TTFB, Duration) □ User Sessions
Collected Entities	☑ URLs ☑ Countries ☑ Client IP Addresses ☑ Client Subnets ☑ Response Codes ☑ User Agents ☑ Methods ☑ OS and Browsers

7. Scroll to the bottom and click **Finished**

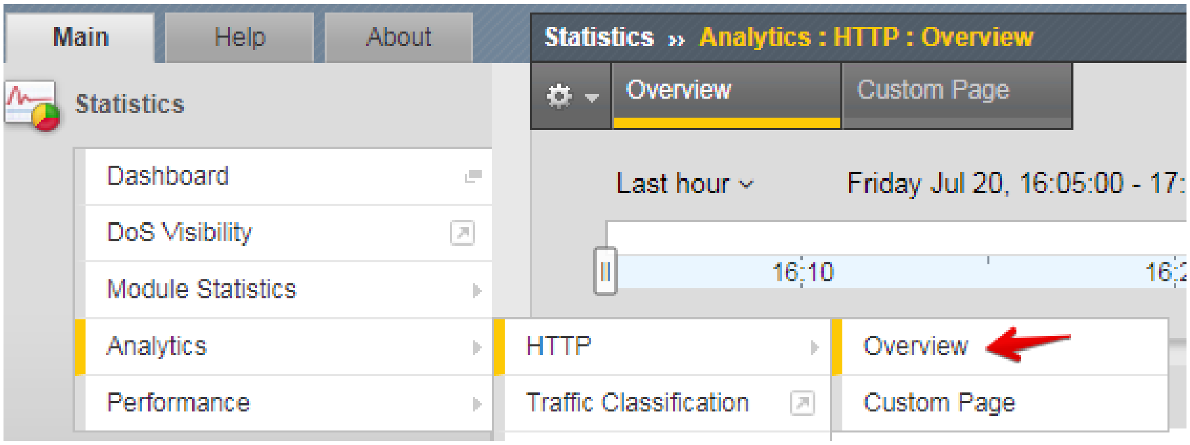
You have now configured your BIG-IP device to collect analytics data and start processing it.

Note: Please note that it typically takes 5-10 minutes for the system to start analyzing the data. Please wait at least 5 minutes before proceeding to the next task.

2.2 Viewing the Analytics data

Once we have had some traffic received by the application Virtual Servers and processed by the Analytics profile, we can now go in to view and analyze this data.

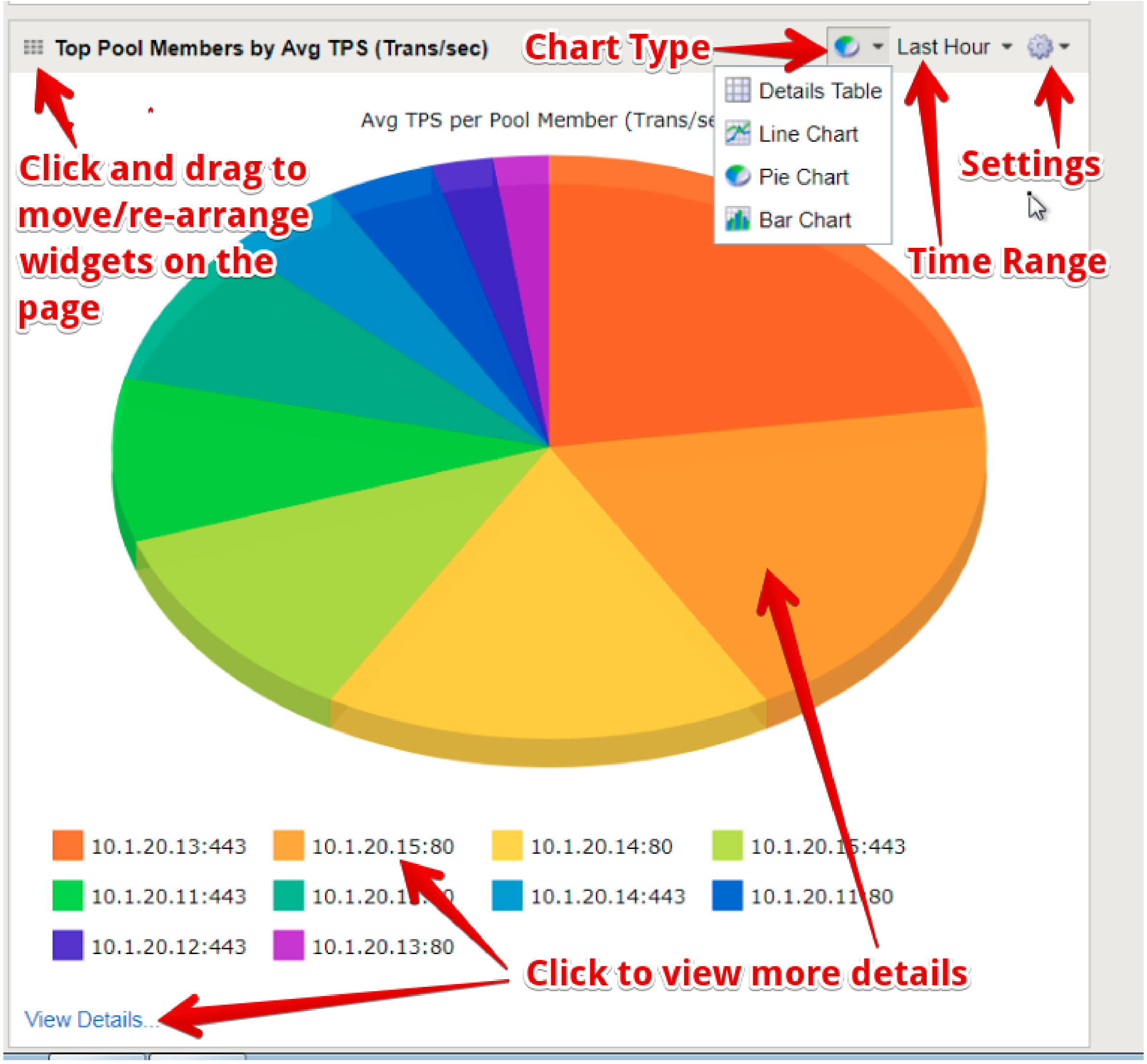
1. In the BIG-IP GUI, go to **Statistics** >> **Analytics** >> **HTTP** >> **Overview**



2. This page shows you details about the traffic received by every Virtual Servers that had the HTTP Analytics profile attached.

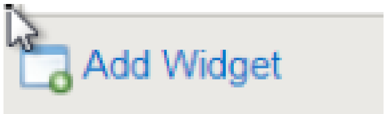
3. You can filter and update the graphs, by selecting one or more **Virtual Servers** from the filters on the right. Selecting one or more Virtual Servers will update the graphs to show data only for the selected Virtual Servers. You can also choose from other filter options, like **Pool Members**, **URLs**, **Client IP Addresses**, etc. Feel free to explore the various graphs and filter options on your own.

4. You can also go to the the **Statistics** >> **Analytics** >> **HTTP** >> **Custom Page**, and customize the various widgets shown.

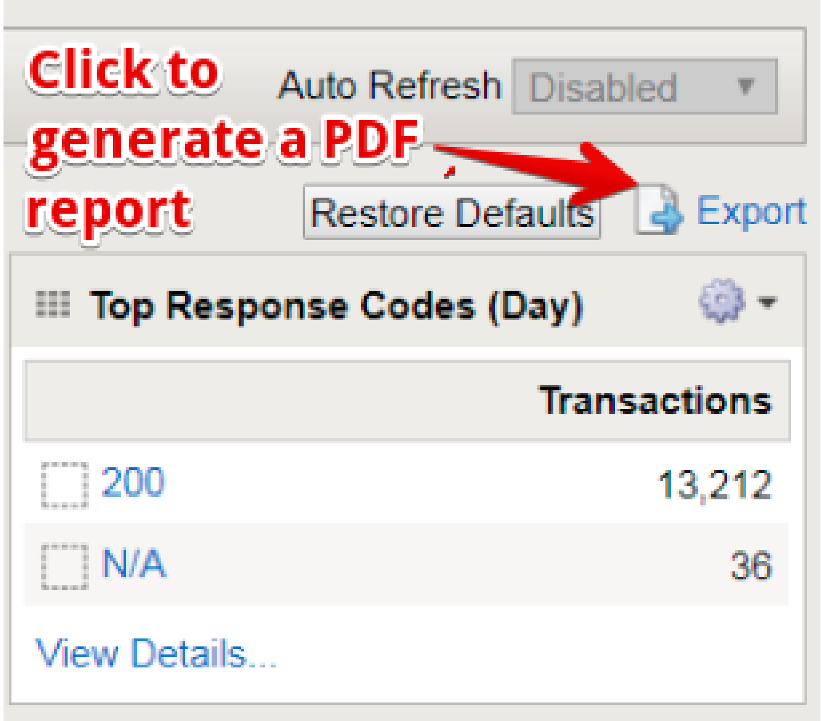


5. You can move the widgets around and re-arrange the page by simply dragging-and-dropping the widgets from the top-left corner of each widget. add more widgets on the page by clicking the **Add Widget** button at the bottom of the page.

6. Similarly, you can modify the tables on the right side of the page, and add another table by clicking the **Add Widget** button below the last table on the right.



7. Once you have updated the page to show you the data you want, you can create a report by clicking the **Export** button at the top-right of the page.



Click to generate a PDF report

Auto Refresh Disabled

Top Response Codes (Day)

	Transactions
200	13,212
N/A	36

8. We encourage you to explore the different widgets and graphs on the page, and change the settings on each to view and analyze the data by various metrics.

3 Lab 2: Integration with Splunk

Splunk is a 3rd-party Security Information and Event Management (SIEM) solution that is used by a large number of organizations to assimilate information and event logs from a large number of disparate sources, and store and analyze it from a single central location in order to correlate data across all devices in the organization.

In this lab, we will integrate our BIG-IPs to send data into Splunk and use Splunk to visualize and analyze the data from a single centralized location rather than viewing/analyzing it on an individual BIG-IP.

3.1 Configuring Splunk to use the F5 Splunk app

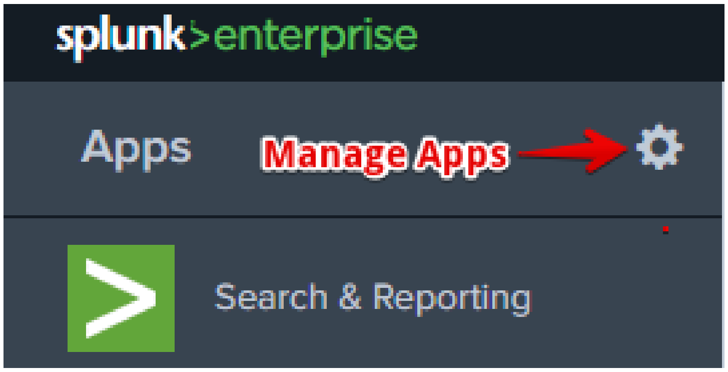
In order to get Splunk to process and display Analytics data from your BIG-IPs, you need to configure it to accept this data, parse and process it, and display it in a meaningful way for you to get the most out of it. In order to help with this, F5 has collaborated with Splunk to create a Splunk app that is available as a free add-on to your Splunk deployment. This F5 Analytics Splunk app can be downloaded from the Splunkbase web-site here:

https://apps.splunk.com/apps/id/f5

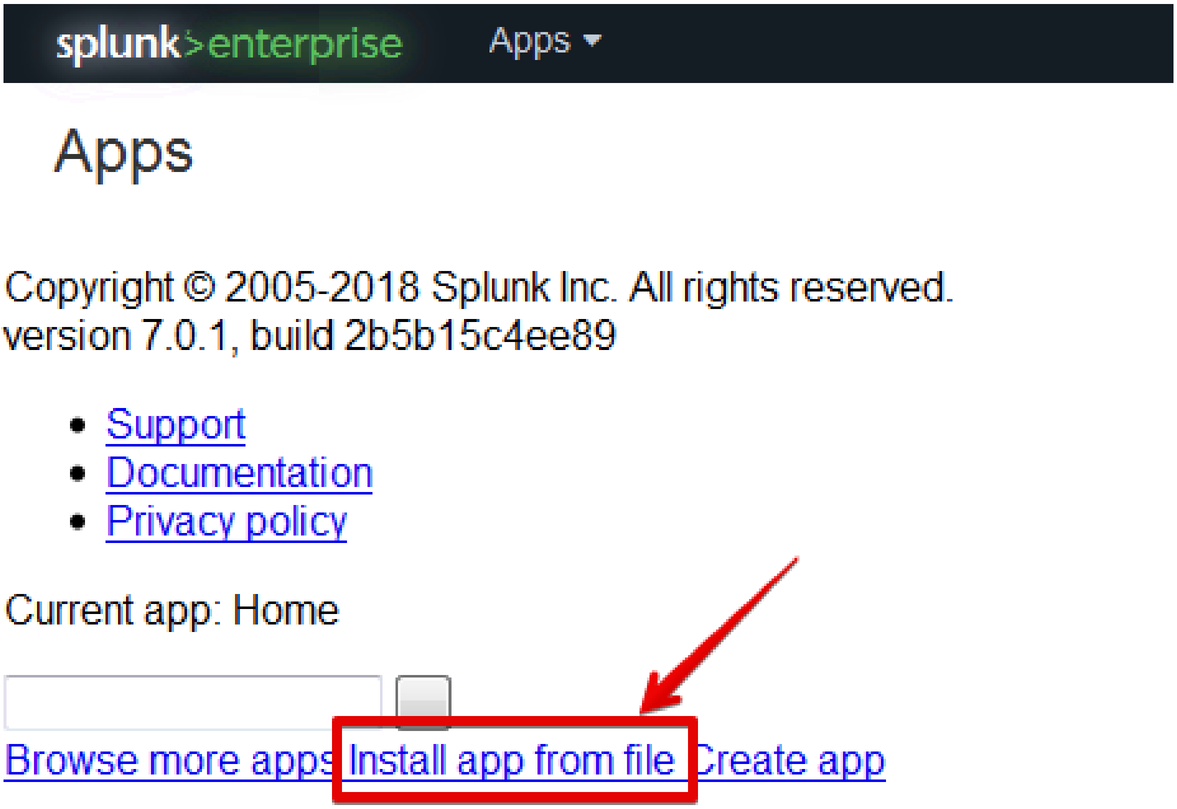
Note: For your convenience, we have already downloaded this Splunk app onto the Windows jump box, so we can just go ahead and install it within our Splunk instance.

3.1.1 Task 1: Install the F5 Splunk app in Splunk

1. In the Chrome browser on your Windows jump box, click the bookmark for **Splunk** to launch the Splunk web UI
2. On the Splunk Enterprise splash page, if you are prompted for an update, click **Skip update**
3. In the Splunk Web GUI, click on the settings button next to **Apps** (on the left) to **Manage Apps**



4. Click **Install app from file**

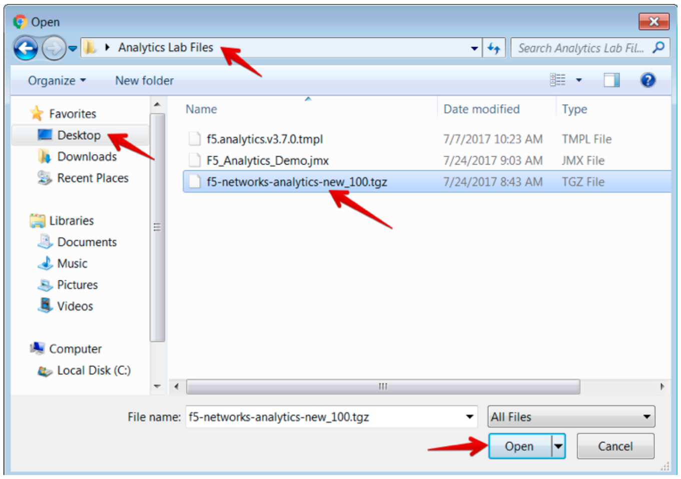


Copyright © 2005-2018 Splunk Inc. All rights reserved.
version 7.0.1, build 2b5b15c4ee89

- Support
- Documentation
- Privacy policy

Current app: Home

5. Click **Choose File**
6. In the file browser window, navigate to **Desktop > Analytics Lab Files,** and choose the **f5-networks-analytics-new_100.tgz file** and click **Open**

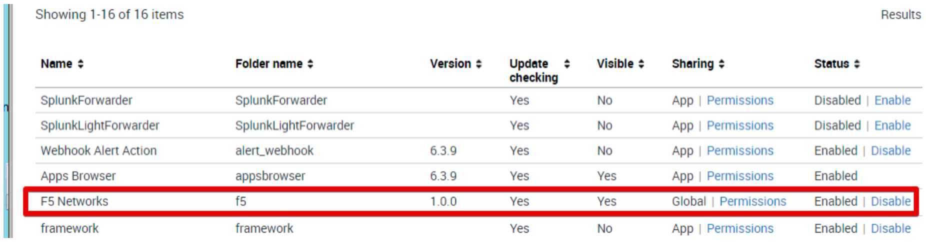


Name	Date modified	Type
f5.analytics.v3.7.0.tmpl	7/7/2017 10:23 AM	TMPL File
F5_Analytics_Demo.jmx	7/24/2017 9:03 AM	JMX File
f5-networks-analytics-new_100.tgz	7/24/2017 8:43 AM	TGZ File

File name: f5-networks-analytics-new_100.tgz

7. Click **Upload**

8. Once the upload is complete, you should see the **F5 Networks** app listed in the Apps table, with the Status set to **Enabled**

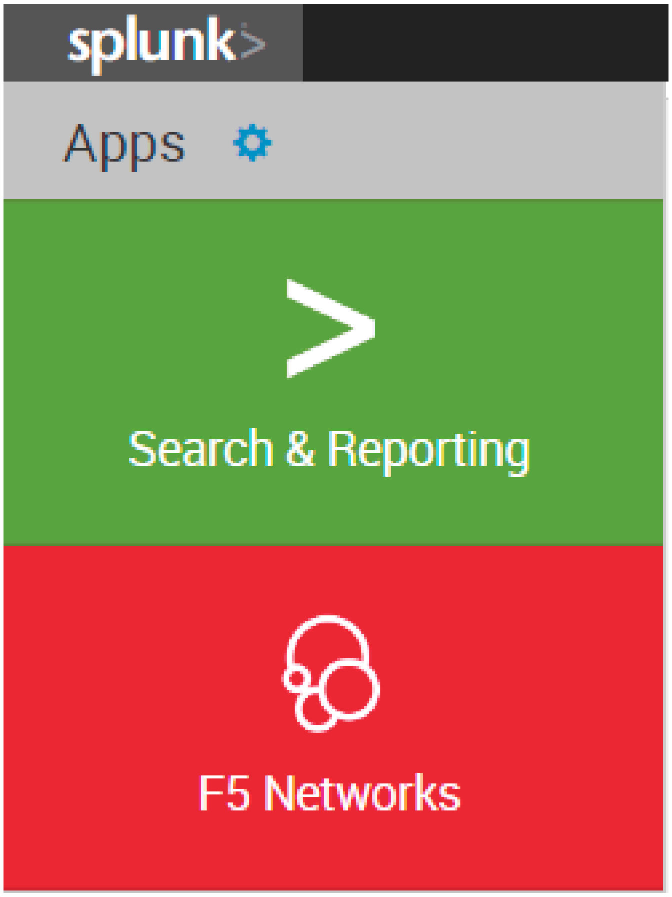


Showing 1-16 of 16 items

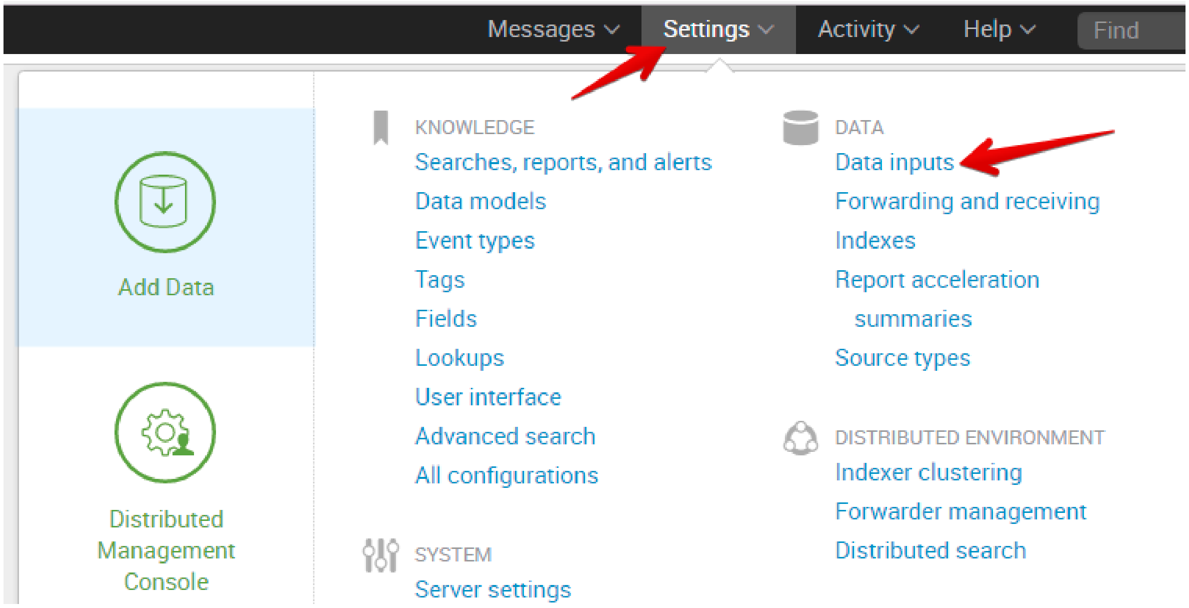
Results

Name ⇕	Folder name ⇕	Version ⇕	Update checking ⇕	Visible ⇕	Sharing ⇕	Status ⇕
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable
Webhook Alert Action	alert_webhook	6.3.9	Yes	No	App | Permissions	Enabled | Disable
Apps Browser	appsbrowser	6.3.9	Yes	Yes	App | Permissions	Enabled
F5 Networks	f5	1.0.0	Yes	Yes	Global | Permissions	Enabled | Disable
framework	framework		Yes	No	App | Permissions	Enabled | Disable

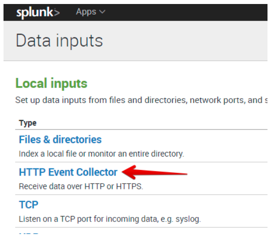
9. Click the **Splunk** logo in the top-left to go to the start page. You should now see the **F5 Networks** app listed on the left



10. Now click the **Settings** menu in the top-right, and choose **Data inputs**



11. Click on **HTTP Event Collector**



splunk> Apps

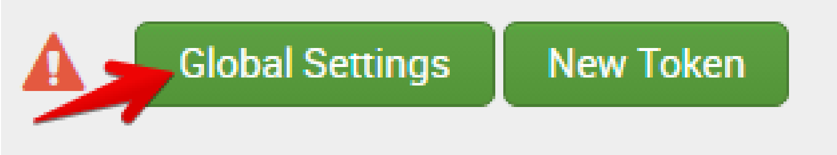
Data inputs

Local inputs

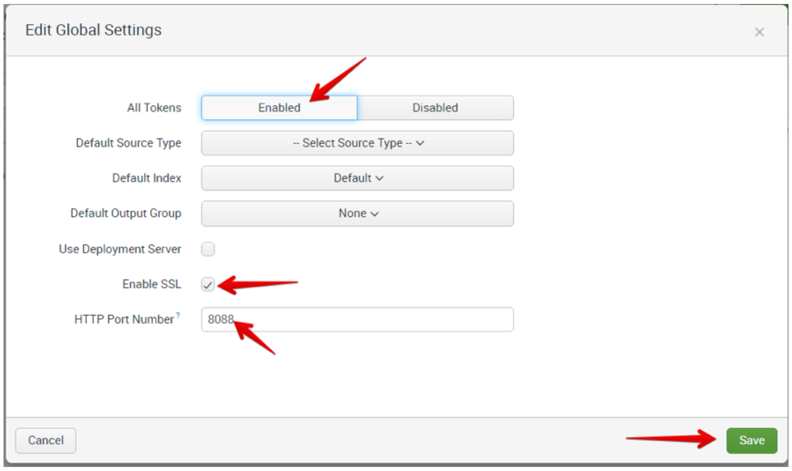
Set up data inputs from files and directories, network ports, and s

Type
Files & directories Index a local file or monitor an entire directory.
HTTP Event Collector Receive data over HTTP or HTTPS.
TCP Listen on a TCP port for incoming data, e.g. syslog.

12. Click on **Global Settings** in the top-right



13. In the Edit Global Settings window:
    - Click on **Enabled** for **All Tokens**
    - Ensure that **Enable SSL** is checked
    - Ensure that **HTTP Port Number** is set to **8088**
    - Click **Save**

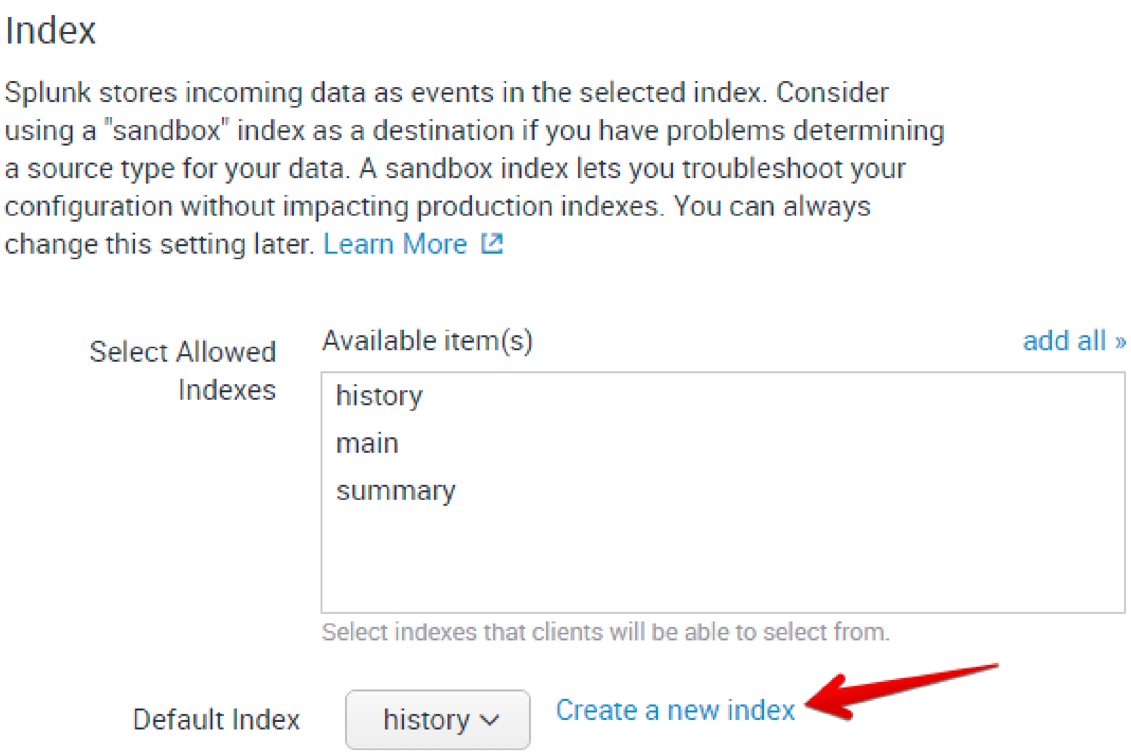


Edit Global Settings

All Tokens	[✓ Enabled] Disabled
Default Source Type	-- Select Source Type --
Default Index	Default
Default Output Group	None
Use Deployment Server	□
Enable SSL	☑
HTTP Port Number ?	8088

Note: Ensure that all of the above settings are exactly as shown, otherwise no data will show up in Splunk.

14. Click **New Token** in the top-right
15. For the Name, enter **F5-Analytics**, and then Click **Next >** at the top
16. On the **Input Settings** page, scroll down till you see **Default Index**, and then click the **Create a new index** link



Index

Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Select Allowed Indexes — Available item(s) — add all »

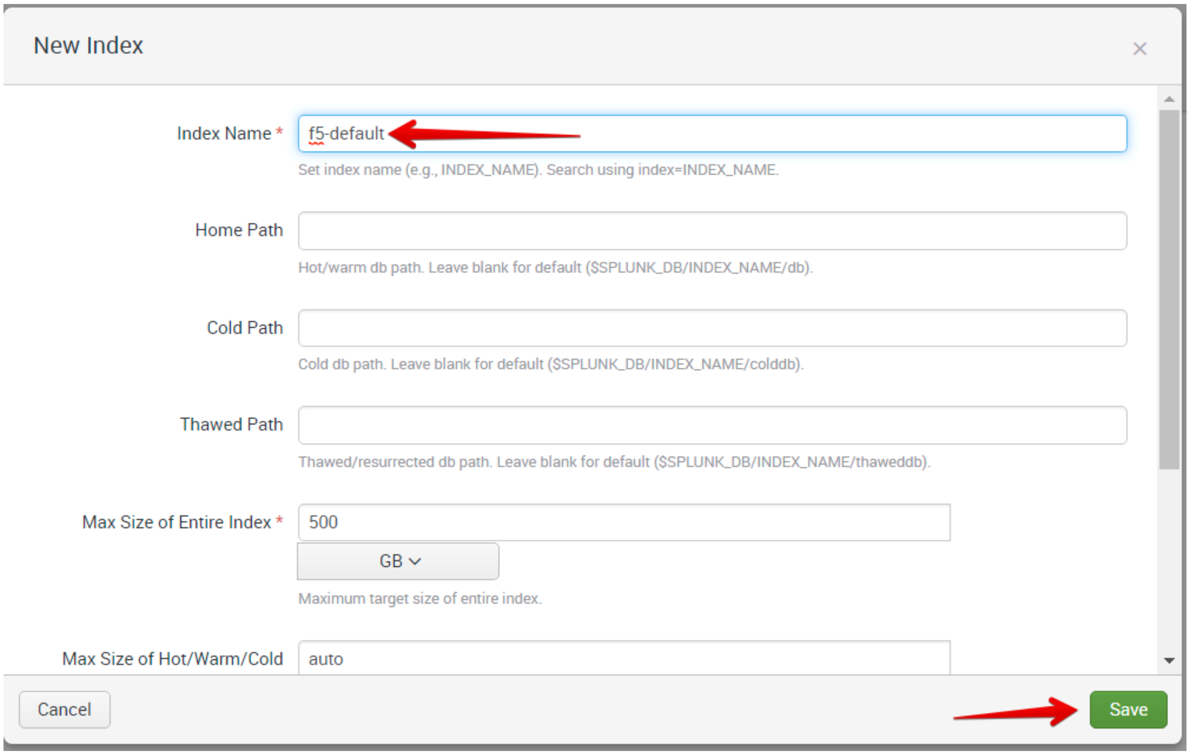
- history
- main
- summary

Select indexes that clients will be able to select from.

Default Index: history

Create a new index

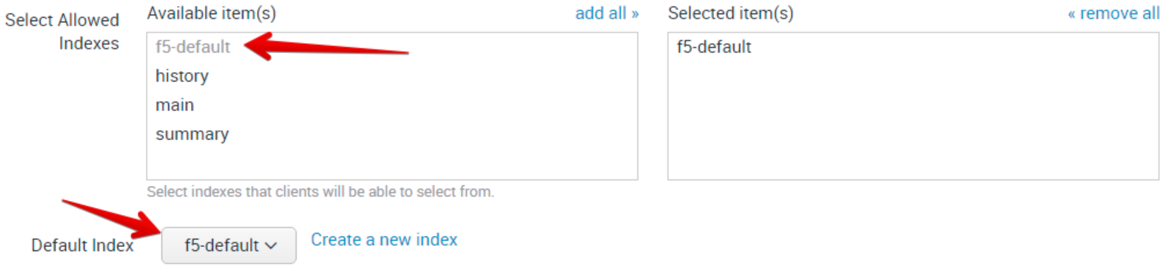
17. In the **New Index** window, enter **f5-default** for the **Index Name**, and click **Save**



New Index

Index Name *	f5-default
	Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.
Home Path	
	Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).
Cold Path	
	Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).
Thawed Path	
	Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).
Max Size of Entire Index *	500 GB
	Maximum target size of entire index.
Max Size of Hot/Warm/Cold	auto

18. In the **Select Allowed Indexes** table, click **f5-default** to move it to **Selected item(s)**



Select Allowed Indexes

Available item(s): f5-default, history, main, summary

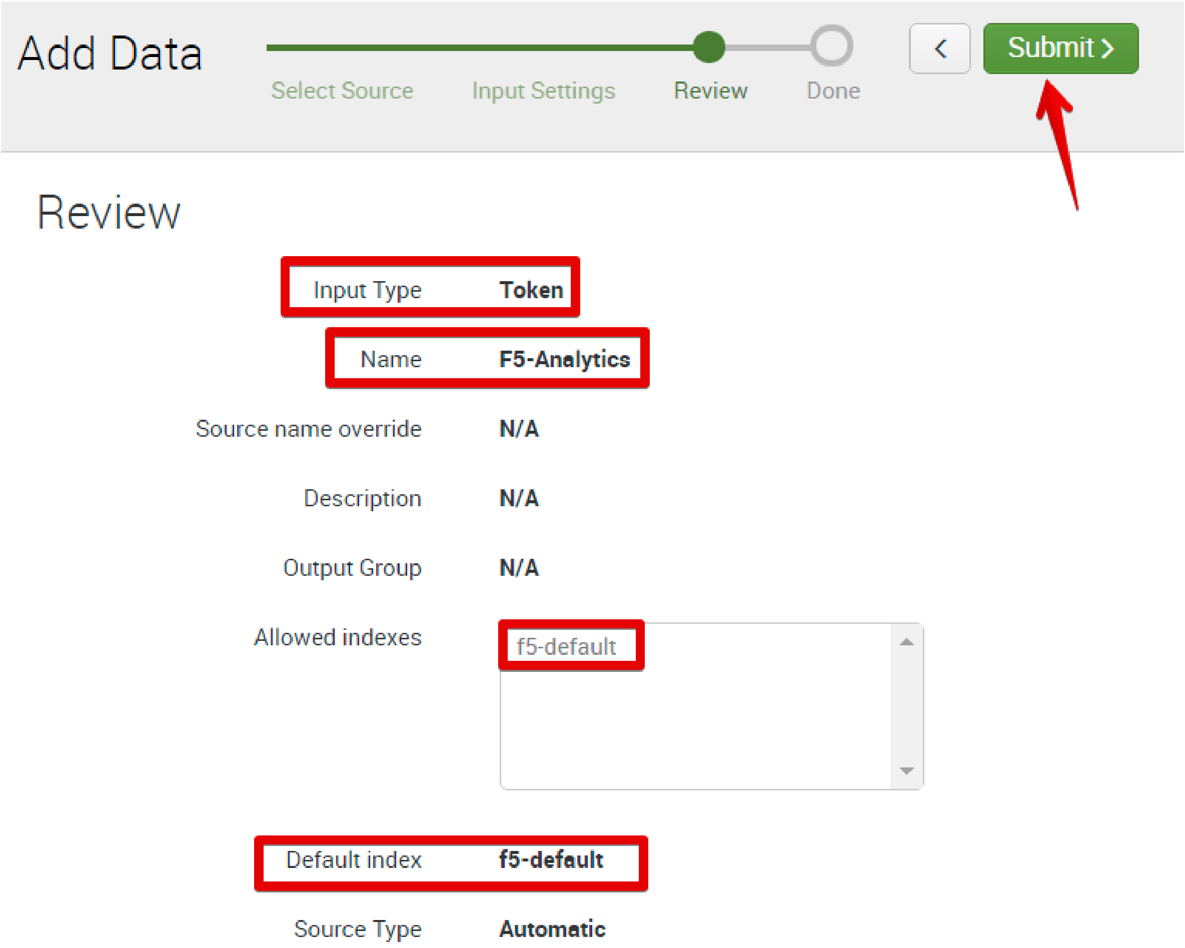
Selected item(s): f5-default

Select indexes that clients will be able to select from.

Default Index: f5-default

19. Click **Review** at the Top

20. Ensure your settings match those shown in the screenshot below, then click **Submit**



Review

Input Type: Token

Name: F5-Analytics

Source name override: N/A

Description: N/A

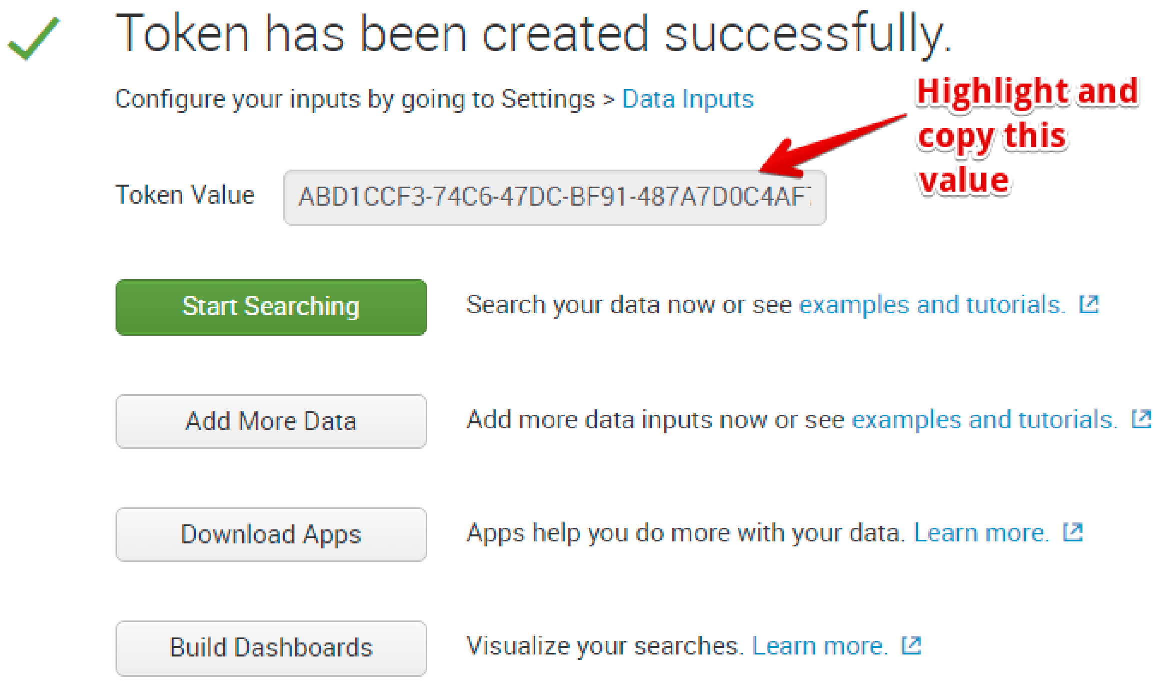
Output Group: N/A

Allowed indexes: f5-default

Default index: f5-default

Source Type: Automatic

21. Once your token has been created, highlight the **Token Value** for the newly created Token, and copy it to your clipboard (**Ctrl-C** or **Right-click > Copy**). We will use this later.



Token has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Token Value: ABD1CCF3-74C6-47DC-BF91-487A7D0C4AF

Highlight and copy this value

Search your data now or see examples and tutorials.

Add more data inputs now or see examples and tutorials.

Apps help you do more with your data. Learn more.

Visualize your searches. Learn more.

Note: Your token value will be different from the one shown above

22. Click on the **Splunk** logo in the top-left to go back to the Splunk start page.

3.2 Configuring the BIG-IP to send analytics data to Splunk

F5 has created an iApp that simplifies the process of configuring your BIG-IP to send Analytics data to remote sources (including Splunk and/or BIG-IQ). There is also a deployment guide that walks you through the steps needed to configure the iApp.

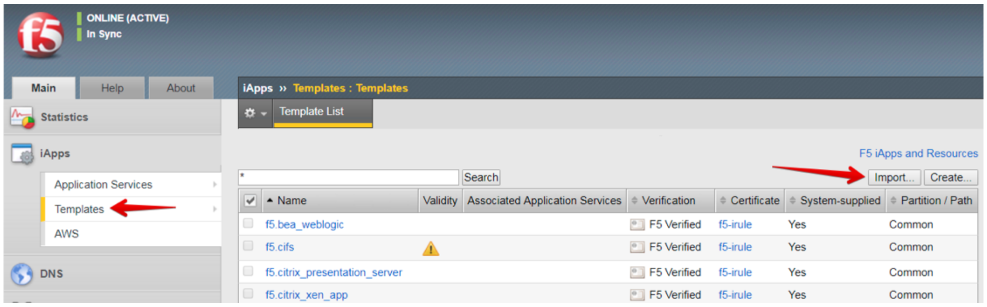
- Details about the iApp and deployment guide can be found on the Ask F5 Support site here: https://support.f5.com/csp/article/K07859431
- You can also find a high-level overview of the iApp, as well as some additional resources (including demo videos of the Splunk integration) on the following F5 DevCentral page: https://devcentral.f5.com/codeshare/f5-analytics-iapp

Note: The F5 Analytics iApp template itself does not ship with the product, but can be downloaded from the F5 downloads site (https://downloads.f5.com).

For your convenience, we have already downloaded the iApp template on the Windows jump box, so we can just import it into our BIG-IP.

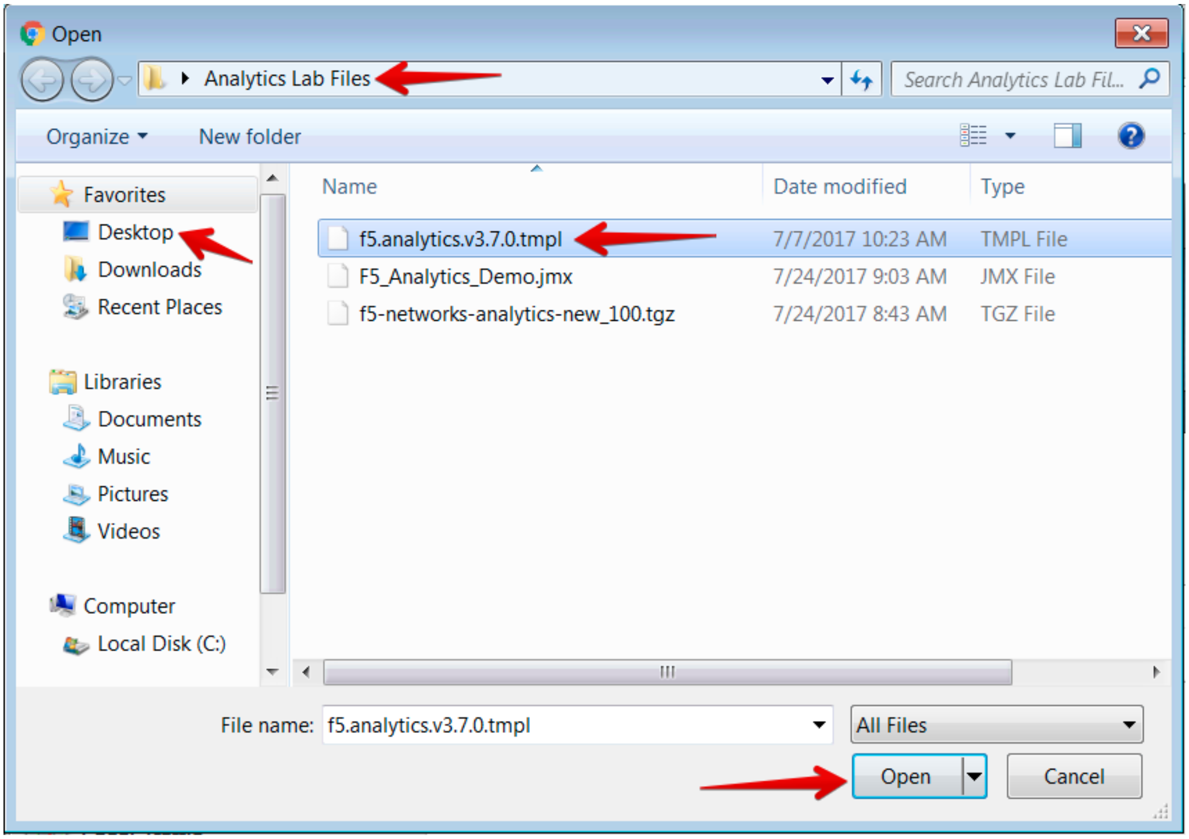
3.2.1 Task 2: Import and configure the F5 Analytics iApp template on the BIG-IP

1. Open a new tab in your Chrome browser, and click on the bookmark for **BIGIP_A** to connect to the BIG-IP GUI
2. Login using the following credentials:
   - Username: `admin`
   - Password: `Agility2018`
3. Go to **iApps >> Templates**
4. Click **Import** in the top-right



☑	Name	Validity	Associated Application Services	Verification	Certificate	System-supplied	Partition / Path
□	f5.bea_weblogic			F5 Verified	f5-irule	Yes	Common
□	f5.cifs	⚠		F5 Verified	f5-irule	Yes	Common
□	f5.citrix_presentation_server			F5 Verified	f5-irule	Yes	Common
□	f5.citrix_xen_app			F5 Verified	f5-irule	Yes	Common

5. Click **Choose File**
6. Navigate to **Desktop > Analytics Lab Files**, and select the **f5.analytics.v3.7.0.tmpl** file. Click **Open**

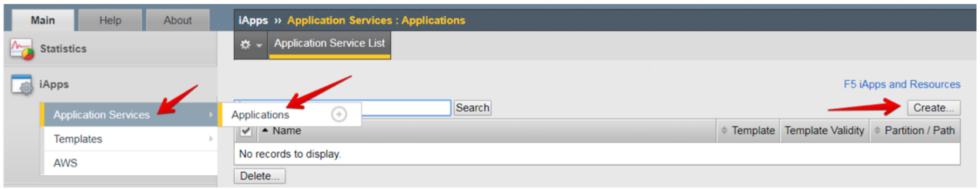


Name	Date modified	Type
f5.analytics.v3.7.0.tmpl	7/7/2017 10:23 AM	TMPL File
F5_Analytics_Demo.jmx	7/24/2017 9:03 AM	JMX File
f5-networks-analytics-new_100.tgz	7/24/2017 8:43 AM	TGZ File

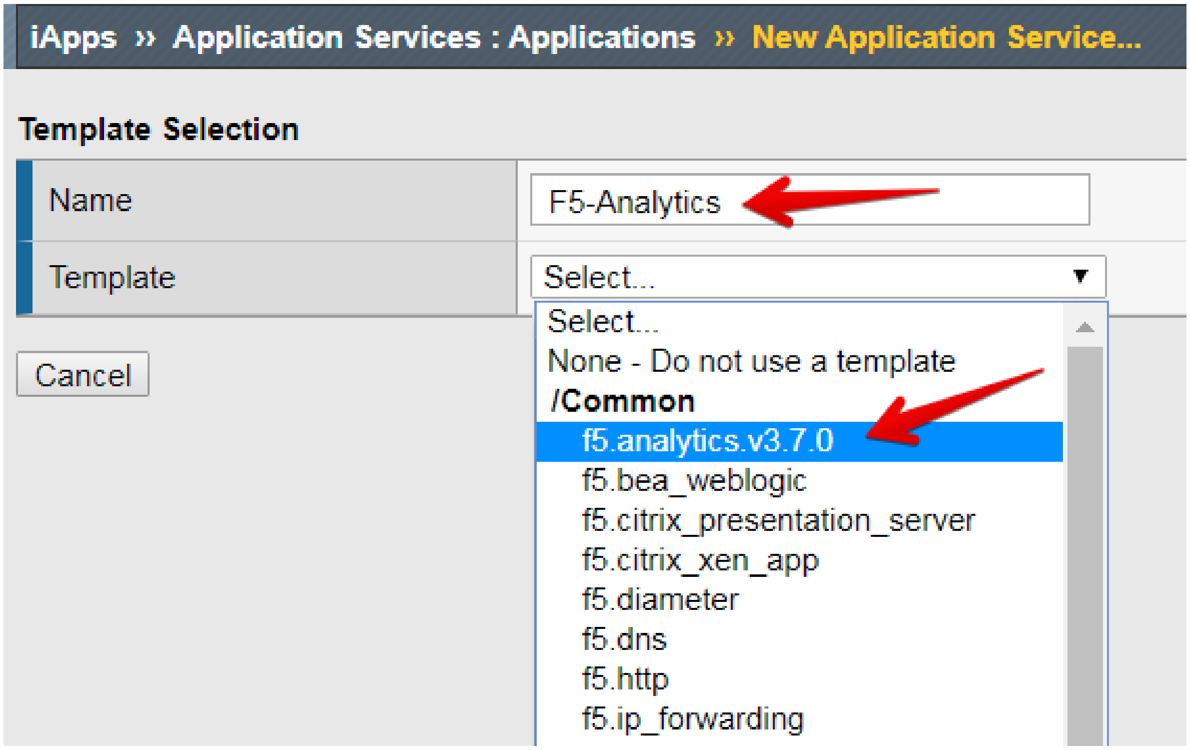
File name: f5.analytics.v3.7.0.tmpl

7. Click **Upload**

8. Once the file is finished uploading, you should see it listed in the iApp Templates table.
9. Go to **iApps >> Application Services >> Applications**
10. Click **Create** in the top-right



11. For the **Name**, enter `F5-Analytics`
12. From the **Template** pull-down menu, choose **f5.analytics.v3.7.0**

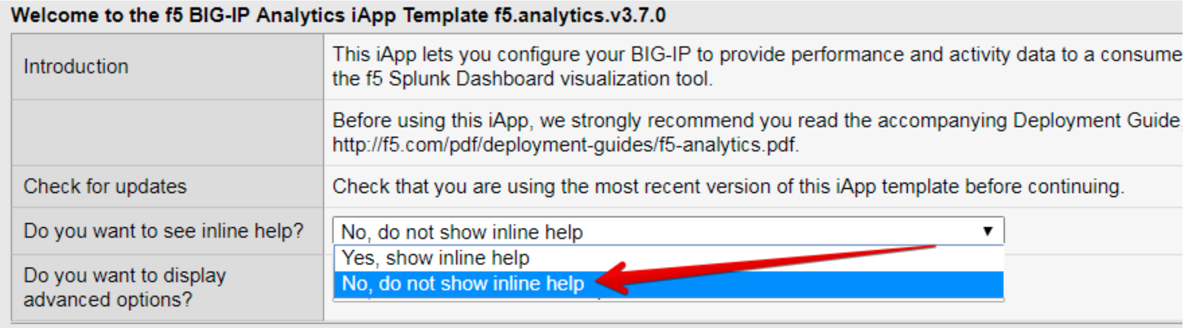


iApps » Application Services : Applications » New Application Service...

Template Selection

Name	F5-Analytics
Template	Select...

13. In the template configuration, in the **Welcome to the f5 BIG-IP Analytics iApp Template** section, change the response for the **Do you want to see inline help?** Question to **No, do not show inline help.**



Welcome to the f5 BIG-IP Analytics iApp Template f5.analytics.v3.7.0

Introduction	This iApp lets you configure your BIG-IP to provide performance and activity data to a consume the f5 Splunk Dashboard visualization tool.
	Before using this iApp, we strongly recommend you read the accompanying Deployment Guide http://f5.com/pdf/deployment-guides/f5-analytics.pdf.
Check for updates	Check that you are using the most recent version of this iApp template before continuing.
Do you want to see inline help?	No, do not show inline help
Do you want to display advanced options?	

Note: If you are not familiar with what all the different settings refer to, you may want to keep the inline help enabled. For now, we have disabled it just to reduce the amount of additional text on the configuration screen.

14. Under the **Information Sources** section, set the following:

    (a) Data Format: **Splunk**

    (b) System Statistic: **Yes**

    (c) Module High Speed Logging Streams: **Yes**

    (d) Local System Logging (syslog): **Yes**

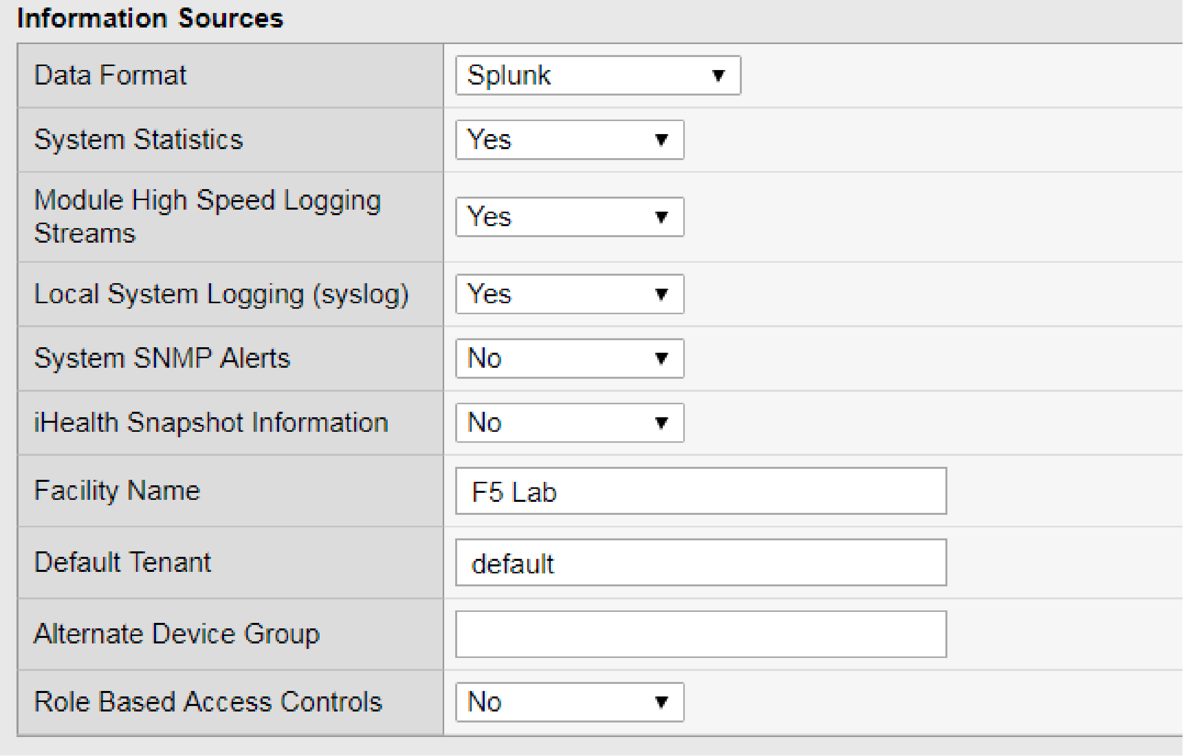
    (e) System SNMP Alerts: **No**

    (f) iHealth Snapshot Information: **No**

    (g) Facility Name: `F5 Lab`

    (h) Default Tenant: `default`

    (i) Role Based Access Controls: **No**



Information Sources

Data Format	Splunk ▼
System Statistics	Yes ▼
Module High Speed Logging Streams	Yes ▼
Local System Logging (syslog)	Yes ▼
System SNMP Alerts	No ▼
iHealth Snapshot Information	No ▼
Facility Name	F5 Lab
Default Tenant	default
Alternate Device Group	
Role Based Access Controls	No ▼

15. Under the **Analytics System Configuration**, enter the following:

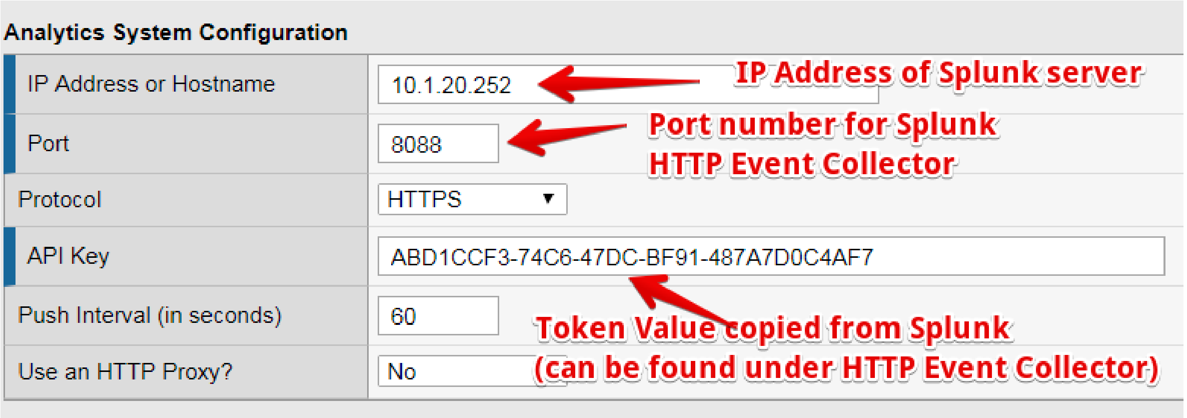
    (a) IP Address or Hostname: `10.1.20.252`

    (b) Port: `8088`

    (c) Protocol: **HTTPS**

    (d) API Key: *<paste the Token Value that you copied from Splunk in the previous task>*

    Leave other settings at their default values



Analytics System Configuration

IP Address or Hostname	10.1.20.252
Port	8088
Protocol	HTTPS ▼
API Key	ABD1CCF3-74C6-47DC-BF91-487A7D0C4AF7
Push Interval (in seconds)	60
Use an HTTP Proxy?	No

IP Address of Splunk server

Port number for Splunk HTTP Event Collector

Token Value copied from Splunk (can be found under HTTP Event Collector)

16. Leave all settings under **Module Log Stream Capture** and **Local Logging Capture** sections at their default values

17. Under **Application Mapping**, leave all settings at their default values, *except* in the Mapping Table, enter the following:

    (a) Order: `10`

    (b) Type: **App Name**

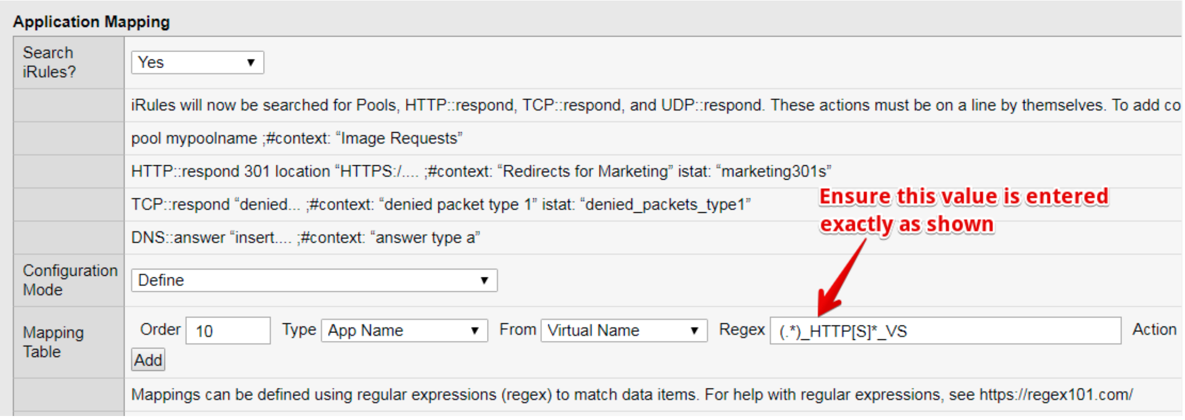
    (c) From: **Virtual Name**

    (a) Regex: `(.*)_HTTP[S]*_VS`

    (b) Action: **Map**

    (c) AppendPrefix: *<leave blank>*

    (d) DirectMapping: *<leave blank>*



Application Mapping

Search iRules?	Yes ▼
	iRules will now be searched for Pools, HTTP::respond, TCP::respond, and UDP::respond. These actions must be on a line by themselves. To add co
	pool mypoolname ;#context: "Image Requests"
	HTTP::respond 301 location "HTTPS:/.... ;#context: "Redirects for Marketing" istat: "marketing301s"
	TCP::respond "denied... ;#context: "denied packet type 1" istat: "denied_packets_type1"
	DNS::answer "insert.... ;#context: "answer type a"
Configuration Mode	Define ▼
Mapping Table	Order 10 Type App Name ▼ From Virtual Name ▼ Regex (.*)_HTTP[S]*_VS Action Add
	Mappings can be defined using regular expressions (regex) to match data items. For help with regular expressions, see https://regex101.com/

Ensure this value is entered exactly as shown

4. Click **Finished**

Note: It may take up to 10 minutes for the system to start showing data in Splunk.

3.3 Notes on the F5/Splunk Integration

While you wait for the data to be generated and for Splunk to gather and analyze the data, here is some additional information to help you understand how the integration between F5 and Splunk works, and what kind of information it can provide.

3.3.1 F5.analytics iApp on BIG-IP

This iApp template is designed to gather a large number of statistics and event information from a variety of different sources, and export the data to different kinds of data collectors / SIEM systems. The sources of information that the iApp gathers include system performance metrics (CPU, memory usage, throughput, connection rates, etc.), tmstats (statistics collected by the Traffic Management Microkernel / TMM regarding the traffic that is being handled/processed by TMM), event logs (from the /var/log directory), SNMP trap-related information, and AVR data (detailed HTTP and TCP stats). Note that the AVR module does NOT need to be enabled in order to export the AVR data via this iApp. Also, the configuration options in the iApp allow the user fine-grained control on what data will be collected and bundled up to be sent to external receivers.

The iApp also provides the ability to customize the output format for different receivers, including F5 BIG-IQ, Splunk, as well as other 3rd-party systems. Furthermore, the iApp provides for options to group together and/or map different pieces of information (Virtual Servers and their associated objects, etc.) into Facilities (e.g. data centers), tenants (for multi-tenant environments), and applications, where a single application could consist of multiple virtual servers (for example, a web application could consist of both, an HTTP and an HTTPS virtual server that serve the same application). This application mapping can also be applied across multiple BIG-IPs so that the same application hosted in different locations can be grouped together under a single application name.

For more details on the iApp, please see the iApp Deployment Guide, which can be found here:

https://www.f5.com/pdf/deployment-guides/f5-analytics-dg.pdf

3.3.2 F5 Networks Splunk App for Splunk

Splunk is a very popular Security Information and Event Management (SIEM) system that has the ability to accept statistics and event data from a large variety of sources, and visualize and display it in a meaningful way to allow an end-user to be able to view events and metrics across multiple devices from a single-pane-of-glass view. Additionally, Splunk allows add-on applications to be integrated into the Splunk deployment in order to allow customized processing and display of data from various sources. The F5 Networks Splunk app is just such an add-on that was created by F5 in partnership with Splunk to allow customized processing of data from F5 BIG-IP devices, and to produce easy-to-use dashboards that analyze and present the data in meaningful charts and graphs.

The data presented in the F5 Networks Splunk app includes a lot of data that cannot be easily visualized on a BIG-IP, such as tmstats information, virtual server and pool member health stats, system performance information, and even syslog event information. Additionally, this app provides the ability to collate and present data across multiple BIG-IP devices, even BIG-IPs in different locations, allowing a user to view all their devices and their data in one single central location, rather than having to view it separately on each individual BIG-IP device.

3.3.3 Configuration options for F5.analytics iApp and the F5 Networks Splunk app

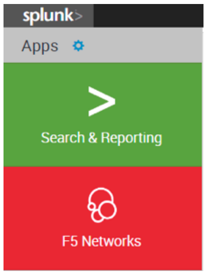
Note that this lab guide walks you through some simple setup options for both, the Splunk app as well as the iApp, in order to help you get up-and-running quickly. However, these configuration options are by no means the only way to configure these. To get a better understanding of all the configuration options we ask that you refer to the F5 analytics iApp deployment guide referenced above, which also has a section on configuring the Splunk app.

3.4 Viewing the Analytics Data in Splunk

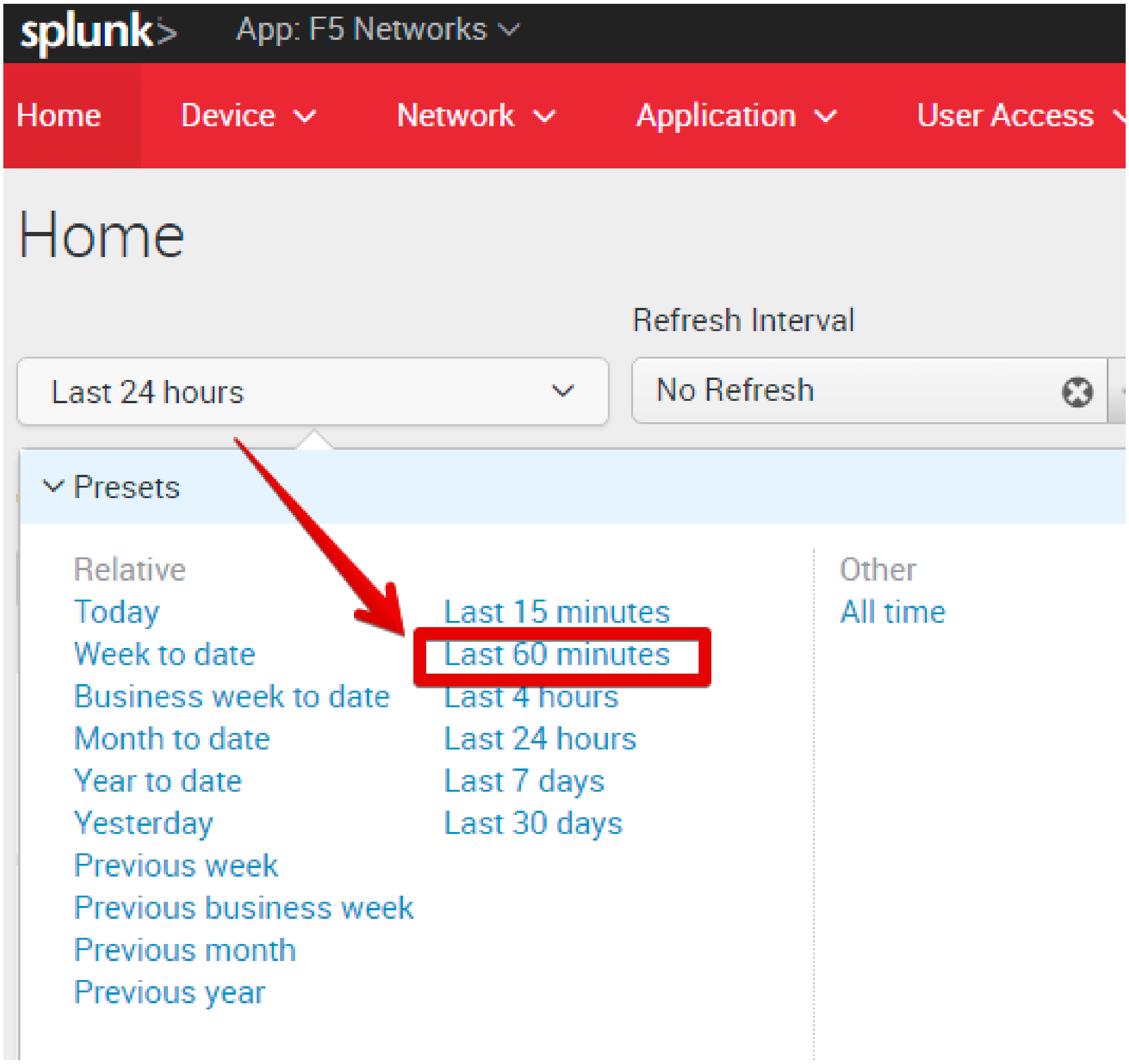
3.4.1 Task 3: Visualize the analytics data in Splunk

Note: It typically takes up to 10 minutes for the system to start showing data in Splunk after you have configured the BIG-IP to send data to it. Please ensure you have waited at least 10 minutes after completing the previous task before you start viewing the data in Splunk.

1. In your Chrome browser window, open a new tab, and click on the **Splunk** bookmark to launch the Splunk Web UI
2. In Splunk, click on the F5 Networks app on the left to launch the F5 Splunk app

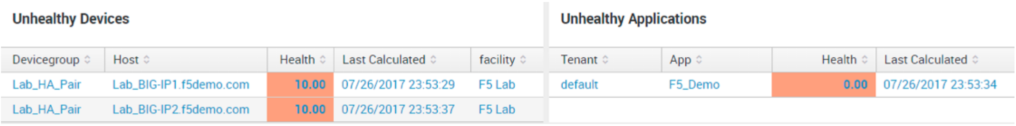


3. On the Home tab of the F5 Splunk app, change the Time pull-down to **Last 60 minutes**



4. Note that some of the widgets like **Non-Responding Hosts** or **Expiring SSL Certificates** may show **No results found**. This is because there is nothing to report for these metrics in this lab environment.

5. Scroll down to view other widgets. You may find that your BIG-IP devices are shown under the **Unhealthy Devices** and/or some applications are shown in the **Unhealthy Applications.** Let's investigate:



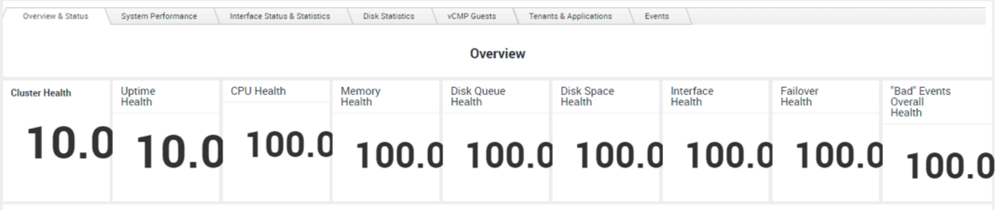
Unhealthy Devices

Devicegroup	Host	Health	Last Calculated	facility
Lab_HA_Pair	Lab_BIG-IP1.f5demo.com	10.00	07/26/2017 23:53:29	F5 Lab
Lab_HA_Pair	Lab_BIG-IP2.f5demo.com	10.00	07/26/2017 23:53:37	F5 Lab

Unhealthy Applications

Tenant	App	Health	Last Calculated
default	F5_Demo	0.00	07/26/2017 23:53:34

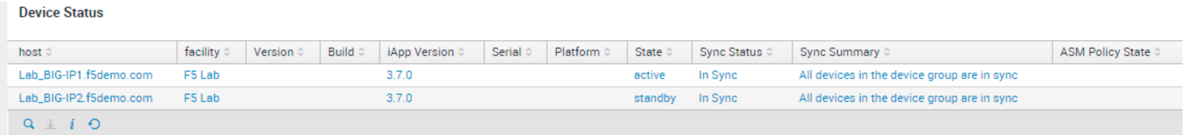
6. Click on the **F5_SJC_Cluster** device group under **Unhealthy Devices.** This will open a new browser tab and take you to the **Device Cluster Drilldown** dashboard. Here you can see a number of different metrics that contribute to the overall device health score.



Overview

Cluster Health	Uptime Health	CPU Health	Memory Health	Disk Queue Health	Disk Space Health	Interface Health	Failover Health	"Bad" Events Overall Health
10.0	10.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0

7. Just under the **Overview** table showing the scores on different metrics, you can also see a table showing the **Device Status**, with details on the devices included in the group

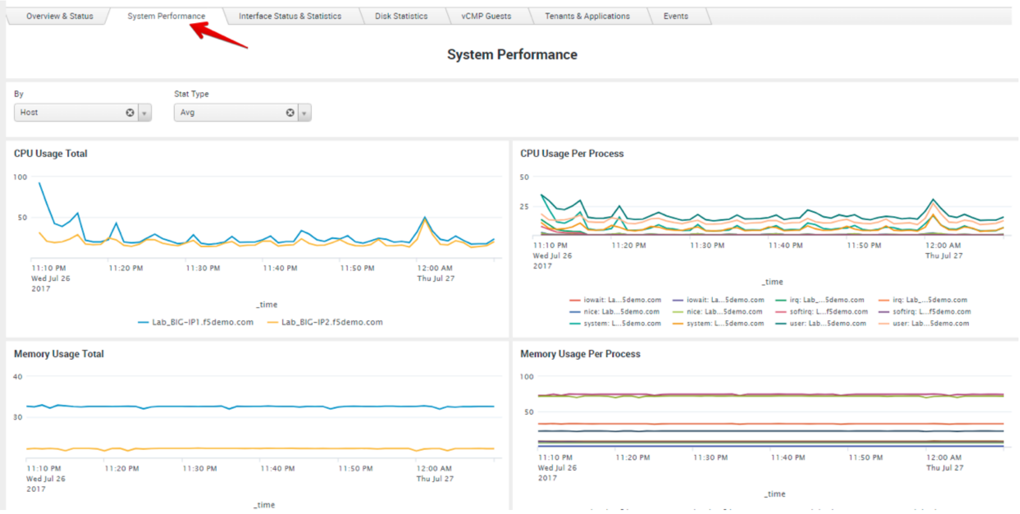


Device Status

host	facility	Version	Build	iApp Version	Serial	Platform	State	Sync Status	Sync Summary	ASM Policy State
Lab_BIG-IP1.f5demo.com	F5 Lab			3.7.0			active	In Sync	All devices in the device group are in sync	
Lab_BIG-IP2.f5demo.com	F5 Lab			3.7.0			standby	In Sync	All devices in the device group are in sync	

8. If your devices had any error conditions that generated some Diagnostic information, you could see that in the **Diagnostics** section.

9. Now click on the **System Performance** tab. This will show you details on the CPU and Memory usage of your BIG-IP devices, including a breakdown of processes consuming the most amount of CPU or memory

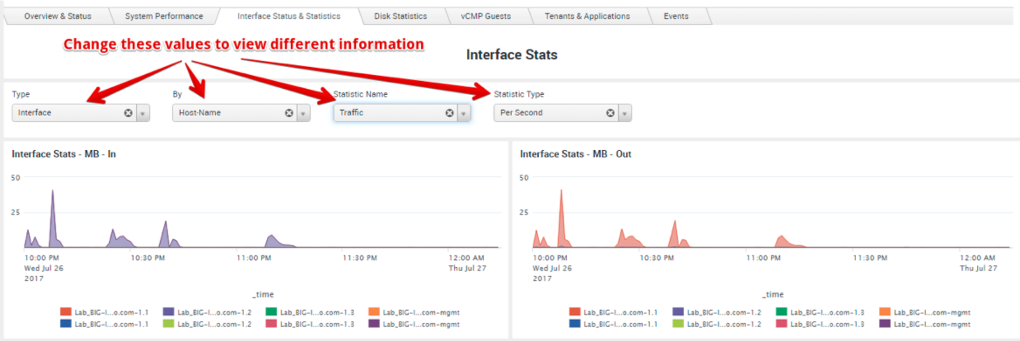


System Performance

By: Host

Stat Type: Avg

10. Next, click on **Interface Status & Statistics**. This will show you detailed Interface and VLAN stats. You can change the options in the pull-down menus to view different information.



Change these values to view different information

Interface Stats

Type: Interface

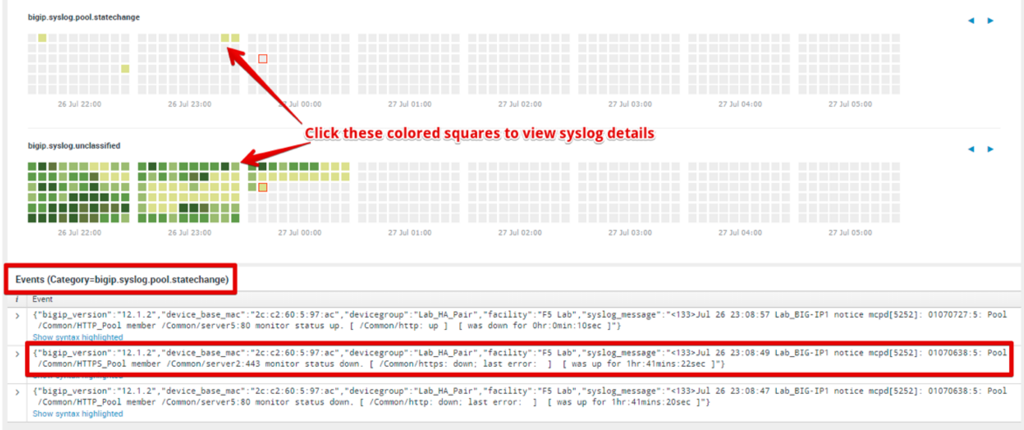
By: Host-Name

Statistic Name: Traffic

Statistic Type: Per Second

11. Next, click on the **Events** tab. This tab shows you Syslog events, with a time-chart of when different kinds of events occurred. If you see any colored squares in the bigip.syslog.pool.statechange syslog

table, click on those squares. If you then scroll down, you will see the actual syslog messages from whatever was happening at that time

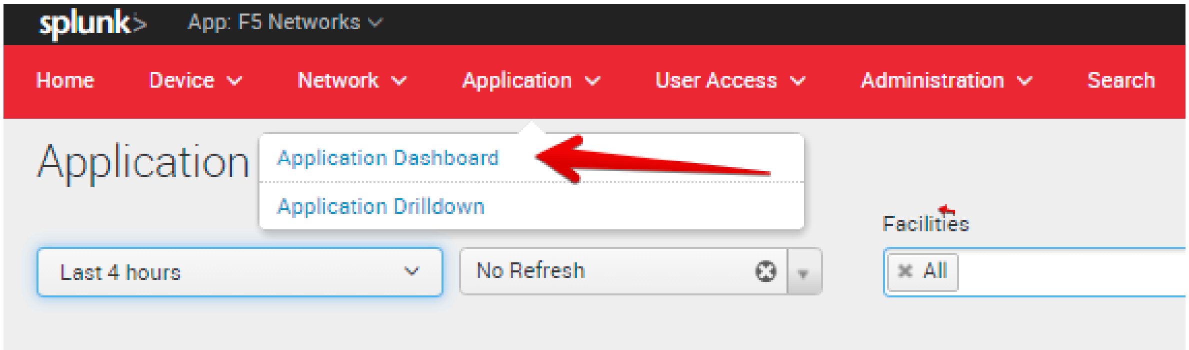

bigip.syslog.pool.statechange
26 Jul 22:00
26 Jul 23:00
27 Jul 00:00
27 Jul 01:00
27 Jul 02:00
27 Jul 03:00
27 Jul 04:00
27 Jul 05:00
Click these colored squares to view syslog details
bigip.syslog.unclassified

Events (Category=bigip.syslog.pool.statechange)

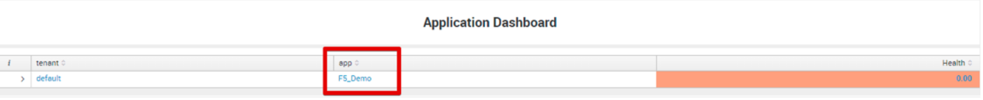
i	Event
>	{"bigip_version":"12.1.2","device_base_mac":"2c:c2:60:5:97:ac","devicegroup":"Lab_HA_Pair","facility":"F5 Lab","syslog_message":"<133>Jul 26 23:08:57 Lab_BIG-IP1 notice mcpd[5252]: 01070727:5: Pool /Common/HTTP_Pool member /Common/server5:80 monitor status up. [/Common/http: up] [was down for 0hr:0min:10sec]"} Show syntax highlighted
>	{"bigip_version":"12.1.2","device_base_mac":"2c:c2:60:5:97:ac","devicegroup":"Lab_HA_Pair","facility":"F5 Lab","syslog_message":"<133>Jul 26 23:08:49 Lab_BIG-IP1 notice mcpd[5252]: 01070638:5: Pool /Common/HTTPS_Pool member /Common/server2:443 monitor status down. [/Common/https: down; last error:] [was up for 1hr:41mins:22sec]"}
>	{"bigip_version":"12.1.2","device_base_mac":"2c:c2:60:5:97:ac","devicegroup":"Lab_HA_Pair","facility":"F5 Lab","syslog_message":"<133>Jul 26 23:08:47 Lab_BIG-IP1 notice mcpd[5252]: 01070638:5: Pool /Common/HTTP_Pool member /Common/server5:80 monitor status down. [/Common/http: down; last error:] [was up for 1hr:41mins:20sec]"} Show syntax highlighted

12. Feel free to explore the other tabs as well to view additional information

13. Now, let us look at our applications to view more details about them. In the red menu bar at the top, click on **Application > Application Dashboard.**



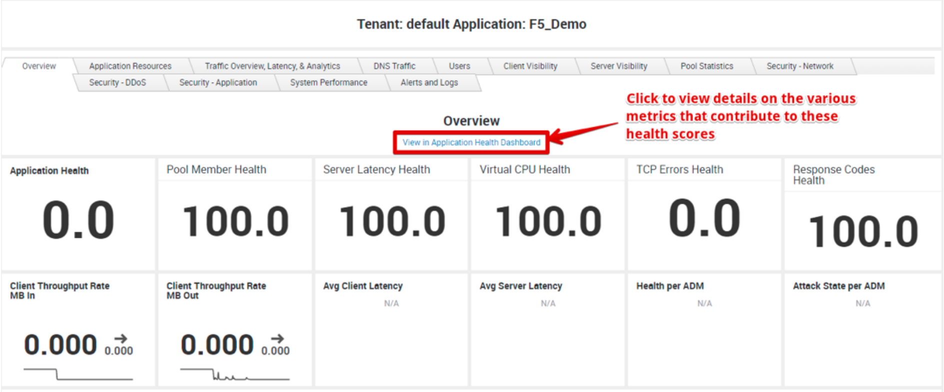
14. This will show you a listing of all the applications across all your BIG-IPs, based on the application grouping and mappings that you defined in the f5.analytics iApp on the BIG-IP. In our case, we just have a single application. Click on the **F5_Demo_App** application name to go into the **Application Drilldown** dashboard



Application Dashboard

i	tenant	app	Health
>	default	F5_Demo	0.00

15. The Application Drilldown dashboard shows you a lot of detailed statistics about your application(s). You can view the various metrics for your application(s) on the **Overview** tab. To get more details, you can click the link for the View in Application Health Dashboard, which will give you even more detailed metrics and charts that are used in calculating the health scores for the various metrics:



Click to view details on the various metrics that contribute to these health scores

16. In the **Application Health** Dashboard that opens up in a new browser tab, you can view the various metrics as well as charts for those metrics that make up the overall Application Health score

17. Now go back to the browser tab for the **Application Drilldown** dashboard, and then click on the **Application Resources** tab. This tab shows you various components that make up your applications, including the facility, virtual servers, pools, pool members, and even iRules. In our case, our **F5_Demo** application is hosted in a single Facility (**F5 Lab**), and is made up of 2 Virtual Servers: **F5_Demo_HTTP_VS** and **F5_Demo_HTTPS_VS**. Each virtual server has its own pool with their corresponding pool members. You can view details for all these components in the tables below.

18. Next, click on the **Traffic Overview, Latency, & Analytics** tab. This tab shows you detailed traffic-related stats, similar to the data available via the AVR charts and reports you saw in Lab 1.

19. Next, click on the **Client Visibility** tab. This tab provides a lot of visibility into the traffic between the end-clients and the BIG-IP, including connection stats, throughput information, TCP stats, HTTP information (HTTP requests, HTTP version, HTTP compression info, etc.), SSL information (SSL throughput, SSL protocol info, ciphers, SSL renegotiations, etc.). Similarly, the **Server Visibility** tab provides similar information for the traffic between the BIG-IPs and the back-end application servers.

20. The **Pool Statistics** tab provides details on the various pools and pool members across all the BIG-IPs and each application / virtual server on each BIG-IP.

21. Feel free to explore other tabs including the **System Performance** and the **Alerts and Logs** tabs.

Note: This concludes all the lab steps for the Splunk Integration lab. Feel free to explore other portions of the F5 Splunk app, or try out other settings in the f5.analytics iApp. Note that this lab environment does not include other F5 modules (DNS/GTM, ASM, or APM). However, if you have these other modules enabled on your BIG-IP devices in your own environment, you can view data for these modules as well in the F5 Splunk app.
